






METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS**Publication number:** WO9712344**Publication date:** 1997-04-03**Inventor:** CURRY STEPHEN M; LOOMIS DONALD W; FOX CHRISTOPHER W**Applicant:** DALLAS SEMICONDUCTOR (US)**Classification:****- International:** G06Q10/00; G06Q20/00; G06Q40/00; G06Q50/00; G07F7/08; G07F7/10; G09C1/00; G06Q10/00; G06Q20/00; G06Q40/00; G06Q50/00; G07F7/08; G07F7/10; G09C1/00; (IPC1-7): G07F7/10; G06F17/60; G07F19/00**- European:** G07F7/08C2; G07F7/08C2B; G07F7/10D4E2; G07F7/10D4T; G07F7/10E**Application number:** WO1996US15471 19960926**Priority number(s):** US19950004510P 19950929; US19960594983 19960131**Also published as:** WO9712344 (A3)
 EP0862769 (A3)
 EP0862769 (A2)
 US6105013 (A1)
 US5748740 (A1)

more >>

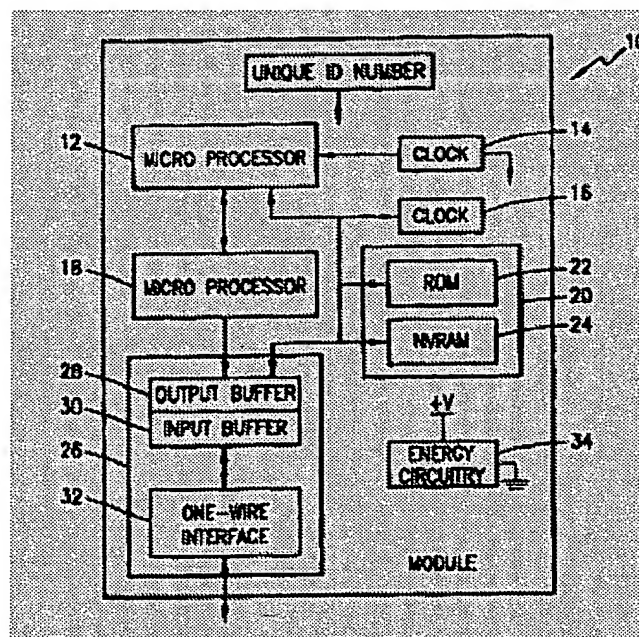
Cited documents: EP0458306
 EP0186981
 EP0194839
 DE4406602
 EP0294248

more >>

Report a data error here

Abstract of WO9712344

The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平11-513509

(43) 公表日 平成11年(1999)11月16日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 19/00		G 0 6 F 15/30	3 6 0
17/60		G 0 7 F 7/10	
G 0 7 F 7/10		G 0 9 C 1/00	6 1 0 C
19/00			6 2 0 B
// G 0 9 C 1/00	6 1 0		6 6 0 B

審査請求 未請求 予備審査請求 有 (全 73 頁) 最終頁に続く

(21) 出願番号 特願平9-513652
(86) (22) 出願日 平成8年(1996)9月26日
(85) 翻訳文提出日 平成10年(1998)3月30日
(86) 国際出願番号 PCT/US96/15471
(87) 国際公開番号 WO97/12344
(87) 国際公開日 平成9年(1997)4月3日
(31) 優先権主張番号 60/004, 510
(32) 優先日 1995年9月29日
(33) 優先権主張国 米国 (US)
(31) 優先権主張番号 08/594, 983
(32) 優先日 1996年1月31日
(33) 優先権主張国 米国 (US)

(71) 出願人 ダラス セミコンダクター コーポレイシ
ョン
アメリカ合衆国75244-3292 テキサス州,
ダラス, サウス ベルトウッド パークウ
エイ 4401
(72) 発明者 カーリイ, スチーブン, エム.
アメリカ合衆国75248 テキサス州 ダラ
ス, クリアヘイブン サークル 6646
(72) 発明者 ルーミス, ドナルド, ダブリュ.
アメリカ合衆国75019 テキサス州 コッ
ペル, ダコタ レーン 316
(74) 代理人 弁理士 浅村 皓 (外3名)

最終頁に続く

(54) 【発明の名称】 安全取引のための方法、装置、システムおよびファームウェア

(57) 【要約】

本発明は、安全取引に使用される電子モジュールに関する。より詳細には、この電子モジュールはマネーおよびその他の有価データを電子的に安全に送ることができるよう、安全な暗号化された技術によりサービスプロバイダの機器の間で情報を送ったり受信したりできる。このモジュールは後に検出できるように、リアルタイムのトラックを維持し、取引を記録し、暗号化鍵のペアを作成するようにプログラムできる。

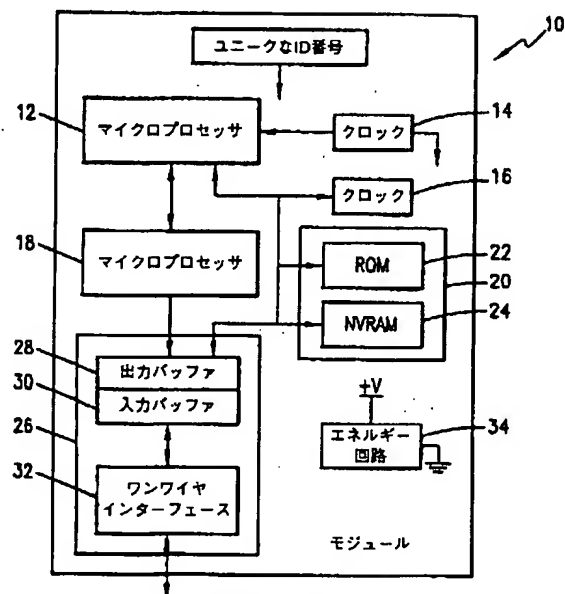


FIG. 1

【特許請求の範囲】

1. データ処理回路と通信するための入出力回路と、
前記入出力回路に電氣的に接続された数値コプロセッサ回路と、
前記入出力回路に電氣的に接続されたマイクロプロセッサ回路と、
前記マイクロプロセッサ回路に電氣的に接続されたメモリ回路とを備え、前記データ処理回路との間で安全な暗号化されたデータの転送を行うようプログラム可能な、安全な取引を行うのに使用される電子モジュール。
2. 前記データ処理回路が別の電子モジュールである、請求項1記載の電子モジュール。
3. 前記入出力回路に接続されたワンワイヤインターフェースを更に備えた、請求項1記載の電子モジュール。
4. 前記メモリ回路が前記電子モジュールと前記データ処理回路の間で暗号化されたデータを転送する間使用するための秘密暗号化／暗号解読鍵を記憶するようになっている、請求項1記載の電子モジュール。
5. 前記暗号化された取引に時間スタンプが押される、請求項1記載の電子モジュール。
6. 第1モジュールおよびサービスプロバイダの機器とを備え、
前記第1モジュールが、
入出力回路と、
乱数を発生するための乱数発生手段と、
乱数を発生し、この乱数を前記入出力回路に与えることを前記乱数発生手段に請求するための第1取引グループとを含み、
前記サービスプロバイダの機器が前記第1モジュールの前記入出力回路からの前記乱数を読み出すための手段と、
前記乱数と第1データとを組み合わせ、前記乱数と前記第1データとの組み合わせを秘密化鍵によって暗号化し、第1の証明書を作成するための手段とを備え、
前記第1モジュールの前記入出力回路が前記第1の証明書を受信するようになっている、安全取引の通信を行うためのシステム。

7. 前記サービスプロバイダの機器が第1のモジュールを含む、請求項6記載のシステム。

8. 前記第1モジュールが、前記第1モジュールを識別するための識別子を更に備え、前記第1取引グループが前記識別子を前記入出力回路に与える請求項6記載のシステム。

9. 前記読み出すための手段が前記第1モジュールの前記入出力回路からの前記識別子を更に読み出すようになっている、請求項8記載のシステム。

10. 前記第1モジュールが第2の取引グループを更に含む、請求項6記載のシステム。

11. 前記モジュールが完了した取引に時間のスタンプを押すための手段を更に含む、請求項6記載のシステム。

12. モジュールとサービスプロバイダの機器との間で暗号化された情報を伝送するための方法において、

- a) 前記モジュールに第1の乱数を発生する工程と、
- b) 前記乱数を前記サービスプロバイダの機器に送る工程と、
- c) 少なくとも前記乱数を前記サービスプロバイダの機器内の秘密鍵により暗号化し、よって証明書を作成する工程と、
- d) 少なくとも前記証明書を前記モジュールに送る工程と、
- e) 前記証明書を前記モジュール内の公開鍵で暗号解読する工程と、
- f) 前記第1乱数と、工程e)の解読された第1の証明書内で発見された数字とを比較し、2つの数字が一致しているかどうかを判断する工程とを備えた、暗号化された情報を伝送するための方法。

13. 工程b)がモジュールの識別子を前記サービスプロバイダの機器に送る工程を更に含む、請求項12記載の方法。

14. 前記サービスプロバイダの機器が別のモジュールである、請求項12記載の方法。

15. 前記方法が単線のバスを含む、請求項12記載の方法。

16. 前記単線バスが実質的にワンワイヤバスである、請求項15記載の方法。

17. モジュールとサービスプロバイダの機器との間で暗号化された情報を伝

送するための方法において、

- a) 前記サービスプロバイダの機器内で第1の乱数を発生する工程と、
- b) 前記乱数を前記モジュールに送る工程と、
- c) 少なくとも前記乱数を前記モジュールの秘密鍵により暗号化し、よって第1の証明書を作成する工程と、
- d) 少なくとも前記第1の証明書を前記サービスプロバイダの機器に送る工程と、
- e) 前記第1の証明書を前記サービスプロバイダの機器内の公開鍵で暗号解読する工程と、
- f) 前記第1乱数と、工程f)の解読された第1の証明書内で発見された数字とを比較し、2つの数字が一致しているかどうかを判断する工程とを備えた、暗号化された情報を伝送するための方法。

18. 前記サービスプロバイダの機器が別のモジュールである、請求項17記載の方法。

19. 前記方法が単線のバスを含む、請求項17記載の方法。

20. 前記単線バスが実質的にワンワイヤバスである、請求項17記載の方法。

。

21. 第1の暗号化されたデータおよび第2の暗号化されたデータを受信する工程と、

前記第1の暗号化されたデータを前記モジュール内に記憶された秘密鍵で解読し、第1の解読鍵を作成する工程と、

前記第1の解読鍵を電子システムに提供する工程と、

前記第2の暗号化されたデータを前記電子システムを介し、前記第1の解読鍵で解読し、よって有効な情報を作成する工程とを備えた、モジュールを使って暗号化されたデータを解読する方法。

22. 前記暗号化されたデータが電子メールメッセージである、請求項21記載の方法。

【発明の詳細な説明】

安全取引のための方法、装置、システムおよびファームウェア

関連出願

本願は、1995年9月29日に提出された米国仮特許出願第60/004,510号の利益を請求するものである。

出願人を本願出願人と同一とする下記の出願は関連する要旨を含み、よって参照によって本願の開示としてここに組み込む。

「値の単位を転送するための方法、装置およびシステム」を発明の名称とし、1996年1月31日に提出された米国特許出願第08/595,014号。

「安全モジュールと別のモジュールとの間で価値情報を転送する方法」を発明の名称とし、1996年1月31日に提出された米国特許出願第08/594,975号。

発明の背景

発明の技術分野

本願は、安全取引のために使用される方法、装置およびファームウェアに関する。特に電子モジュールに基づくシステムでは、少なくとも安全なデータ転送、デジタル署名を行い、またはマネー取引をオーソライズするよう、モジュールを構成できる。

関連技術の説明

現在ではクレジットカードに連動する磁気ストリップを有するクレジットカードは、市場における好ましいマネー取引媒体となっている。カードのユーザーはカードを自動キャッシュマシン、地域の店または銀行へ持って行き、マネー取引を行うことができる。多くの場合、マネー交換を行うのに電話のインターフェースを介してカードが使用される。カードおよびカードのユーザーの識別を助けるのに磁気ストリップカードが使用される。カードによる転送の安全性のレベルは比較的低い。それにも拘わらず、このカードにより、カードの所有者は製品を購入し、負債の支払いをし、異なる銀行口座間でマネーの交換を行うことができる。

これまでに磁気ストリップカードに関して改良がなされてきた。磁気ストリッ

プの代わりにマイクロ回路を備えたカードも作られており、一般にマイクロストリップのようにマイクロ回路を使用してカード読み取り機が取引を行うことができるようになっている。

発明の概要

本発明は好ましくは携帯モジュールとサービスプロバイダの機器との間で暗号化された情報をやり取りするための装置、システムおよび方法に関する。この発明は乱数、例えばSALTを発生し、例えばマネー交換のためのリクエストと共にこの乱数をサービスプロバイダの機器へ送ることができる、ユニークな識別を有するモジュールを含む。次にサービスプロバイダの機器は他の情報と共に（取引のタイプに応じて）秘密鍵または公開鍵を使って乱数を符号化し、この符号化した情報をサインされた証明書としてモジュールへ送り戻すことができる。モジュールはサインされた証明書を受けると、（取引のタイプに応じ）公開鍵または秘密鍵を用いて証明書を解読し、解読した数字と元の乱数とを比較する。更に、両者の数字が同じであれば、リクエストされた取引を安全と見なし、取引を進める。これらモジュールは時間のスタンプを付けることができ、後に検討できるよう、取引に関する情報をメモリに記憶できる。

図面の簡単な説明

添付図面を参照し、次の詳細な説明を読めば、本発明の方法および装置についてより完全に理解できよう。

図1は、モジュールの一実施例のブロック図である。

図2は、取引グループを作成するためのプロセス例である。

図3は、Eメールメッセージを受けるための技術例である。

図4は、公証機能のためのモジュールを作成するための技術例である。

図5は、公証手段としてモジュールを使用するための技術例である。

図6は、マネー取引を行うためのモジュールを作成するための技術例である。

図7は、モジュールを使用してマネー取引を行うための技術例である。

図8は、モジュールを使用してマネー取引を行うための技術例である。

図9は、モジュールを使用してマネー取引を行うための技術例である。

図10は、ネットワークを通してデータを送るための技術例である。

図11は、モジュール内のソフトウェアおよびファームウェアの組織例である。

図12は、モジュールにおけるソフトウェアおよびファームウェアの構成例である。

現在の時点で好ましい実施例の詳細な説明

図1は、本発明の一実施例を含むモジュール10の一例のブロック図を示す。このモジュール回路は1つの集積回路とすることができる。このモジュール10は組み合わせた多数の集積素子回路またはディスクリート素子回路で構成できると理解できよう。このモジュール10はマイクロプロセッサ12と、リアルタイムクロック14と、制御回路16と、数値コプロセッサ(math coprocessor)18と、メモリ回路20と、入出力回路26と、エネルギー回路とを含む。

モジュール10は限定するわけではないが、トークン、カード、リング、コンピュータ、財布、鍵ホルダー(Key fob)、バッジ、宝石、スタンプまたは対象のユーザーが持ったり、および／またはユーザーと連設できる、実質的に任意の物体を含む種々の物体内に組み込むことができるよう充分小さくできる。

マイクロプロセッサ12は8ビットマイクロプロセッサであることが好ましいが、16、32、64または任意の作動可能な数のビットのマイクロプロセッサとすることができる。クロック14はモジュール回路に対するタイミングを定める。連続的に作動するリアルタイムクロックとなるような別個のクロック回路14を設けてもよい。

数値コプロセッサ回路18は極めて大きい数を処理するように設計されており、そのために使用される。特にこのコプロセッサはRSAの暗号化および暗号解読の複雑な数学的処理を行う。

メモリ回路20はリードオンリーメモリと、不揮発性のランダムアクセスメモリの双方を含むことができる。更に当業者であれば、等価的なデバイスを作るのに揮発性メモリ、EPROM、SRAMおよび種々の他のタイプのメモリ回路を使用できることが理解できよう。

制御回路16は回路全体に対するタイミング、ラッチングおよび種々の必要な制御機能を行う。

入出力回路 26 はモジュール 10 との双方向の通信を可能とし、この入出力回路 26 は好ましくは少なくとも 1 つの出力バッファ 28 と、入力バッファとを含む。ワンワイヤバスを介した通信を行うために、この入出力回路 26 と共にワンワイヤインターフェース回路 32 を設けることができる。

メモリ回路 20 を維持し、および／またはモジュール 10 内の他の回路への給電を助けるのに、エネルギー回路 34 が必要である。このエネルギー回路 34 はバッテリーと、コンデンサと、R/C 回路と、光電池と、または他の等価的なエネルギーを発生する回路または手段から構成できる。

次に、安全取引モジュールおよびモジュール 10 を使った一連のサンプルアプリケーションの好ましい実施例のファームウェアアーキテクチャについて説明する。これら例は、モジュール 10 の好ましい特徴の組を説明し、かつモジュールが提供するサービスを説明しようとするものである。これらアプリケーションは本発明の機能を限定するものでなく、むしろその機能のサンプルを明らかにするものである。

1. 好ましい実施例およびそのファームウェア設計の概観

モジュール 10 は、好ましくは汎用の 8051 コンパチマイクロコントローラ 12 または妥当な程度に同様な製品と、連続作動するリアルタイムのクロック 14 と、大きな整数のための高速モジュラー累乗アクセレータ（数値コプロセッサ）18 と、データを送受信するためのワンワイヤインターフェース 32 を備えた入出力バッファ 28、30 と、あらかじめプログラムされたファームウェアを備えた 32 キロバイトの ROM メモリ 22 と、重要なデータを記憶するための 8 キロバイトの NVRAM（不揮発性 RAM）24 と、入力回路 26 内のデータを解釈し、これに作用するようマイクロコントローラ 12 をパワーアップできる制御回路 16 とを含む。モジュール 10 はその作動電力をワンワイヤラインから引き出す。マイクロコントローラ 12 と、クロック 14 と、メモリ 20 と、バッファ 28、30 と、ワンワイヤバスフロントエンド 32 と、モジュラー累乗アクセレータ 18 と、制御回路 16 は、好ましくは 1 つのシリコンチップ上に集積化され、データを破壊することなく NVRAM 24 内のデータをさぐることを実質

的に不可能にさせるパッケージ技術を用い、ステンレススチール製のマイクロカン(microcan)内にパッケージされる。当初は下記に述べるようなアプリケーション

ンをサポートするのに使用するためにNVRAM24のほとんどを利用できる。当業者であればモジュールの構造の相当する変形例が多数あることが理解できよう。例えば揮発性メモリを使用したり、ワンワイヤバスインターフェース以外のインターフェースも使用できる。このシリコンチップはクレジットカード、リング等にパッケージできる。

モジュール10は、好ましくは、最初は有効な機能を奏することができるよう、データをモジュール10にロードするサービスプロバイダによって使用され、次にエンドユーザーの利益のためにサービスプロバイダに代って操作を行うためのコマンドをモジュール10に送るエンドユーザーによって使用されるようになっている。このような理由から、モジュール10は意図するアプリケーションのためにモジュールを設定する際に、サービスプロバイダをサポートするための機能を提供する。更にモジュールはサービスプロバイダが提供するサービスをエンドユーザーが受けることができるようにする機能も提供する。

各サービスプロバイダは取引グループ40を作成することにより、そのサービスをサポートするためのNVRAMメモリのブロックを保留できる(図11~12参照)。取引グループ40とは単にサービスプロバイダによって定義される一組のオブジェクト42である。これらオブジェクト42としては、データオブジェクト(暗号化鍵、取引カウント数、金額、日/時間スタンプ)と、データオブジェクトを有効な方法でどのように組み合わせるかを指定する取引スクリプト44の双方がある。各サービスプロバイダは他のどの取引グループ40とも独立した自己の取引グループ40を作成する。従って、多数のサービスプロバイダは同一のモジュール10内で異なるサービスを提供できる。サポート可能な独立したサービスプロバイダの数は、各取引グループ40内で定義されたオブジェクト42の数および複雑さに応じて決まる。取引グループ40内で定義できるオブジェクト42の一部の例としては次のものがある。

RSAモジュール

クロックオフセット

R S A 指数	ランダム S A L T
取引スクリプト	コンフィギュレーションデータ
取引カウンタ	入力データ

マネーレジスタ	出力データ
デストラクタ	

各取引グループ40内ではモジュール10は最初に取り消し不能な効果を有する所定のコマンドを取り込む。取引グループ40内で一旦これら取り消し不能なコマンドのいずれかが実行されると、これらコマンドはモジュールの有効寿命が終了するまで、またはモジュールが使用する取引グループ40がモジュール10から削除されるまで、有効な状態のままになる。更にモジュールの寿命が終了するまで、またはモジュール10の内容全体を消去するようマスター消去コマンドが発生するまで、取り消し不能な効果を有する所定のコマンドが残される。これらコマンドについては後に更に説明する。

これらコマンドはエンドユーザーが実行できる操作に対する必要な制御をサービスプロバイダに与えるのに基本的なコマンドである。取り消し不能なコマンドの一部の例としては次のものがある。

秘密化オブジェクト	ロックオブジェクト
ロック取引グループ	ロックマイクローインナーA-カン（商標）

モジュールユーティリティの多くは、守秘能力を中心においているので、秘密化コマンドは極めて重要な取り消し不能なコマンドである。

モジュール10が全体としてロックされると、残りのNVRAMメモリ24は今までの取引の監査トレイル（記録）を保持するための特定のバッファのために割り当てられる。取引の各々は取引グループの番号、指定グループ内の取引スクリプト40の番号および日／時間スタンプによって識別される。

ファームウェアによって実行される基本概念は、サービスプロバイダがエンドユーザーに実行できるように望むオブジェクト間の動作だけを実行させるように、取引グループ40内に取引スクリプトを記憶できるようにすることである。サービスプロバイダはサービスプロバイダに代ってモジュール10が取引をサイン

できるようにするRSA鍵(暗号化鍵)を記憶し、秘密化し、よってその認証を保証することもできる。取引グループ40内に1つ以上のオブジェクト42を秘密化および/またはロック(locking)することにより、サービスプロバイダはサービスプロバイダに代ってモジュール10が何をできるようにするかに関する制御

を維持する。エンドユーザーは新しい取引スクリプト44を追加できないので、サービスプロバイダによってプログラムされた取引スクリプト44により実行できるオブジェクト42に対する動作に限定される。

11. モジュールの利用モデル

この章は、最も簡単なことから最も複雑な範囲のモジュール10の一連の実際アプリケーションを示すものである。これらアプリケーションの各々は、どのような理由でモジュール10が、このアプリケーションのための技術を可能にする中心となっているかを明らかにするために、充分詳細に説明する。

A. 安全Eメールの背景

この章では任意のロケーションで誰でも自分のEメールを安全に受け取ることができるようにするのに、どのようにモジュール10を使用できるかの一部を示す。

1. 標準Eメール

標準Eメールシステムではユーザーのコンピュータはインターネットサービスのプロバイダに接続されており、ユーザーのコンピュータは新しいメールを求めてプロバイダのコンピュータを呼び出している際に、ユーザーのコンピュータはEメールのパスワードを与える。Eメールは平文(plain text)のフォームでプロバイダのコンピュータに存在し、ここで働く者がEメールを読む可能性がある。更に発信元から進む間、Eメールは多数のコンピュータを通過し、これらのロケーションで露出される。ユーザーがローカルエリアネットワークを通して自分のプロバイダから自分のメールを受け取った場合、同じネットワーク上の他の者がEメールを捕捉し、読み取る可能性がある。最後に、ユーザーがパスワードを入力しなくてもすむような多数のEメールシステムを使用した場合、ユーザーのコ

ンピュータ側にいる誰でもユーザーのメールを検索し、読み取ることができる。

この理由は、ユーザーのコンピュータがプロバイダのコンピュータを呼び出して
いるとき、ユーザーのコンピュータは自動的にパスワードを送るからである。

ユーザーのコンピュータ内のコンフィギュレーションファイルからパスワード
をコピーし、これを使って別のコンピュータからユーザーの命令を読み取ること
もしばしば可能である。このように平文のフォームでのEメールが広く分散し、

パスワード保護が弱い結果として、標準的なEメールは極めて安全性が低いもの
と考えられる。

この問題を解消するために、P. G. P. (Pretty Good Privacy)として知ら
れる安全システムが考えられた。このP. G. P. を使用するためにユーザーは
公開成分および秘密成分の双方を含む完全なR S A鍵セットを発生する。ユーザ
ーは自分のEメールメッセージすべての署名ブロック内に公開鍵を挿入し、P.
G. P. 公開鍵の公にアクセス可能なダイレクトリ内にこの公開鍵を掲示するこ
とにより、ユーザーの公開鍵を広く利用できるようにする。ユーザーは多分パス
ワードで保護されたフォームで自分のパソコン内に自らの秘密鍵を記憶する。だ
れかがこのユーザーに秘密のEメールを送りたい時にランダムI D E A暗号化鍵
を発生し、このI D E A暗号化アルゴリズムを用いてメッセージ全体を暗号化す
る。次に、意図する受け手により提供される公開鍵を使ってI D E A鍵自体を暗
号化する。次に、I D E Aによって暗号化されたメッセージおよびユーザーの公
開鍵を使って暗号化されたI D E A鍵の双方をユーザーにEメール送信する。こ
の送信を見た者は、送ろうとする相手の受け手を除き、誰もこれを読むことはで
きない。その理由は、このメッセージはI D E Aにより暗号化され、I D E A鍵
は意図する受け手の公開鍵によって暗号化されているからである。受け手のコン
ピュータは対応する秘密鍵を記憶しているので、I D E A鍵を解読し、解読され
たI D E A鍵を使ってメッセージを解読できる。これにより遠隔からユーザーの
メールを読み出そうと試みる者からの安全性が得られるが、ユーザーのコンピ
ュータ自体が秘密鍵を記憶しているので、ユーザーのコンピュータが他のコンピ
ュータにアクセス可能な場合には、これはあまり有効ではない。秘密鍵がパスワー

ドで保護されていても、ユーザーのパスワードを推定したり、またはパスワードの入力時にユーザーを盗み聞きすることは容易であることが多いので、ユーザーのコンピュータは安全性を低くしている。更にユーザーは自分のコンピュータでしか安全なEメールを受信できない。その理由は、ユーザーの秘密鍵を記憶しているのは自分のコンピュータであり、ユーザーの秘密鍵は他の場所では利用できないからである。従って、P. G. P. の弱点は秘密鍵が存在するユーザーのコンピュータに強かに組み合わされていることである。

2. モジュールで保護されたEメール

Eメールを保護するのにモジュール10が使用されている場合、ユーザーはEメールが他人によって読まれたり、または自分のパソコンがEメールの安全性を危うくするような、弱いリンクとなるような恐れなく、ユーザーが行く場所でユーザーに自分のEメールを送ることができる。このモジュールで保護されたEメールシステムはP. G. P. システムと類似するが、パソコン内ではなく、モジュール10の取引グループ内の秘密化オブジェクト内にIDEA鍵を解読するのに使用される秘密鍵が記憶されている点が異なっている。このモジュールで保護されたEメールシステムは次のように作動する。

a. 図2、11および12を参照すると、ユーザーは取引グループ40を作成し(S1)、RSA鍵セットを発生し(S2)、これを取引グループ40の3つのオブジェクト42(1つはRSAモジュールオブジェクトNであり、2つはRSA指数(exponent)オブジェクトE、Dである)にロードする。ユーザーは次に解読指数Dを秘密化する(S3)。最後に、取引スクリプト44を作成し(S4)、入力データオブジェクト内のデータを取り出し、これをモジュラスNおよび秘密指数Dで暗号化し、この結果を出力データオブジェクト内に入れる。ユーザーは別の取引スクリプト44が追加されないようにグループをロックする(S5)。ユーザーはDの値を「忘れ」、公開ディレクトリおよび自分のEメールメッセージの署名ブロック内にEおよびNの値を公開する。ユーザーはDを忘れており、Dの指数オブジェクトは秘密にされているので、だれかがDの値を見つけることはない。

b. 図3を参照すると、ユーザーに安全なEメールを送るのにP. G. P. システムが使用される。ユーザーが安全なEメールを受けると(A1)、ユーザーは暗号化されたIDEA鍵を取引グループ40の入力データオブジェクトへ送り(A2)、次に取引スクリプト44をコールし、この鍵を解読し(A3)、解読された結果を出力データオブジェクトへ入れる(A4)。次にユーザーは、出力データオブジェクトから解読されたIDEA鍵を読み出し、これを使って自分のメールを解読する(A5)。ここで、モジュール10を物理的に所有することなく、ユーザーを含むだれかが新しいメールを読むことは、この時点では不可

能であることに留意されたい。従って、Eメールを読むコンピュータにはモジュール10が物理的に存在していなければならないので、ユーザーに無断でユーザーのメールを読み出す方法はない。ユーザーは自分が行く場所に自分のモジュール10を携帯し、これを使ってどんな場所でも、送られて来たメールを読むことができる。このように、ユーザーの家のコンピュータが安全システムにおける弱点とはならない。

上記のような安全なEメールは、1つのRSA鍵と1つの取引スクリプト44しか必要としない最も簡単な、可能なモジュールアプリケーションである。モジュール10内に公開鍵Eを記憶することも必要がなく、公開鍵は公にアクセス可能と考えられるので、このようにすることはうまいやり方である。指数オブジェクト内に公開鍵Eを記憶し、そのオブジェクトすなわちモジュラスオブジェクトNを秘密化しないことにより、ユーザーはモジュール10から常時公開鍵を読み出すことができるように保証できる。モジュール10は暗号化を実行する必要はないので、公開鍵Eに関連する取引スクリプト44はない。

B. デジタル公証サービス

この章は、モジュール10を使った好ましい公証サービスを説明するものである。

1. 標準公証サービスの背景

従来の公証サービスプロバイダはエンドユーザーからの文章を受信し、これを

検査し、所定の日に公証人にその文書が提示されたことを証明する偽造不能なマークを文書に付ける。かかる公証サービスの1つの利用法として、必要な場合に裁判所で発明の優先権を後に主張できるよう、新しい発明の開示を記録することがある。この場合、公証人によって提供される最も重要なサービスは、所定の日に発明者の所有物としてその開示物が存在していたことを証明することである。

(優先権を決める従来の方法は、重要な発明の開示物に発明者と証人がサインし、日付を記載した研究ノートを用いることである。)

2. モジュールを使用した電子公証サービス

会社（以下サービスプロバイダと称す）は、顧客（以下エンドユーザーと称す）に対する公証サービス（厳密には優先権証明サービス）を行うビジネスに

参入すると決定する。このサービスプロバイダはモジュール10をそのエージェントとして使用することにより、このサービスを行うことと、サービスプロバイダに代って文章を認証する（日付を記載し、サインする）権限をエージェントに与える。このシステムの好ましい作動は次のとおりである。

a. 図4、11および12を参照すると、サービスプロバイダはモジュール10の「登録されたロット」における電子公証機能を行うための取引グループ40を作成する（B1）。

b. サービスプロバイダは安全な計算施設を使ってRSA鍵セットを発生し、3つのオブジェクト42のセット、すなわちモジュラスオブジェクトと2つの指数オブジェクトとして各モジュール10へRSA鍵セットをプログラムする（B2）。鍵セットの公開部分はできるだけ広く知られるようにされており、秘密部分はサービスプロバイダによって完全に忘れられている。秘密指数オブジェクトはモジュール10から読み戻されることがないように秘密にされる。

c. サービスプロバイダは各モジュール10からリアルタイムクロック14を読み出し、リアルタイムクロック14の読み出しと適当な基準時間（例えば1970年1月1日12:00 am）との間の差を含むクロックオフセットオブジェクトを作成する。リアルタイムクロックにこのクロックオフセットオブジェクトの値を加えることにより、任意のモジュール10から真の時間を得るこ

とができる（B3）。

d. サービスプロバイダは0に初期化された取引シーケンスカウンタオブジェクトを作成する（B4）。

e. サービスプロバイダは取引カウンタの値が続き、次にユニークなレーザー登録番号が続く真の時間（クロック14の真のクロックと、クロックオフセットオブジェクトの値の合計）に入力データオブジェクトの内容を添付する、取引スクリプト44を作成する。次にこの取引スクリプト44はこのデータのすべてを秘密鍵で暗号化し、出力データオブジェクト内に入れることを指定する。この動作を実行させる命令は、取引スクリプトオブジェクトとして取引グループ40内に記憶される（B5）。

f. サービスプロバイダは直接読み取り可能、または書き込み可能と

ならないように望む他のオブジェクト42を秘密化する（B6）。

g. サービスプロバイダは取引グループ40をロックし、別の取引スクリプト44が追加されるのを防止する（B7）。

h. 図5を参照すると、次にサービスプロバイダはモジュールを支払い側の顧客（エンドユーザー）に分配し公証サービスに使用する。エンドユーザーが文書を証明させたい時はいつも、エンドユーザーは（安全ハッシュ規格(Secure Hash Standard)、FIPS公開番号180に指定された）安全ハッシュアルゴリズムを実行し、文書全体を20バイトメッセージのダイジェストにまとめる。エンドユーザーは20バイトのメッセージダイジェストを入力データオブジェクトへ送信し（C1）、メッセージダイジェストを、真の時間と、取引カウンタと、ユニークなレーザーシリアル番号と、組み合わせること及びその結果得られたパケットに秘密キーでサインすることを、取引スクリプト44に要求する（C2）。

i. エンドユーザーは証明書を公開鍵で解読し、メッセージダイジェスト、真の時間スタンプ等をチェックし、これらが正しいかどうかを確認するように証明書をチェックする（C3）。次に、エンドユーザーはデジタルフォームで文書のオリジナルコピーと共にこのデジタル証明書を記憶する。サービスプロ

バイダはそのモジュールによって作成された証明書の認証を確認する。

j. サービスプロバイダの指定した時間の後、ユーザーは自分のモジュール10を戻し、料金を払い、新しい秘密鍵を含む新しいモジュールを得る。古いモジュールは取引グループ全体を消去し、これらを再プログラミングすることによりリサイクルできる。サービスプロバイダはこれまで使用した公開鍵のすべてのアーカイブを維持しているので、古い証明書の認証を必要に応じて証明できる。

C. デジタルキャッシュディスペンサ

この使用モデル例は、商品またはサービスに対する支払いを行うことができるキャッシュリザーバとしてのモジュール10に焦点を合わせたものである（説明を簡単にするためにモジュール10にキャッシュを補充することについては、後まで説明を延ばす）。この場合、サービスプロバイダは銀行または金融機関であ

り、エンドユーザーは購入のためにモジュール10を使用したいと考える銀行の顧客であり、業者は購入された商品またはサービスの提供者である。これら取引におけるサービスプロバイダ、業者およびエンドユーザーの役割については後に詳細に説明する。

モジュール10内で実行されるデジタルキャッシュ財布の基本概念は、モジュール10がまず所定のキャッシュ値を含むロックされたマネーオブジェクトを含み、モジュール10がマネーオブジェクトの値からリクエストされた金額を減算した事実を証明する、基本的にサインされた文書である証明証を要求に応じて発生できる概念である。これらサインされた文書は証明書の値に対応する金額だけ内部マネーオブジェクトの値が減少された事実を証明するので、現金に等価的な文書となっている。業者はこれら証明書をサービスプロバイダに戻すことにより、現金でこれら証明書を買い戻すことができる。

現金を表示するデジタル証明書を処理する際に、「再生」(replay)または複製が可能であることが基本的な問題となる。デジタルデータは容易にコピーし、再送信できるので、製造時に使用される特殊な技術によって複製が困難な通常の貨幣または紙幣と異なっている。このような理由から、支払いの受け手は受け取る

デジタル証明書がこれまで発行された証明書の複製でないことを保証するために、特殊な工程をとらなければならない。この問題は、受取人にランダム「SALT」、すなわちチャレンジ番号を発生させ、支払い人にこれを提供させることによって解決できる。

SALTは再生を防止する1つの方法である。チャレンジ/レスポンスモードで乱数を送り、これを使用する。他方の当事者はこれらのレスポンスの一部として乱数を戻すようにチャレンジされる。

支払い人は金額および受取人のSALTの双方を含むサインされた証明書を作成する。受取人がこの証明書を受けると、受取人は公開鍵でこれを解読し、金額をチェックし、支払い人が提供したものとSALTが同じであることを確認する。受取人に対し証明書を秘密にすることにより、支払い人は証明書が複製又は再生でなく、正当なものであることを受取人に対して証明する。この方法は、モジュール10が支払い人か受取人かによらず、使用できる。

解決しなければならない別の問題は、支払いの拒絶ができないことである。このことは、取引への当事者のいずれも、自分が実際に取引に参加していなかったと主張できないことを意味する。取引の記録（マネー証明書）には、取引への各当事者が意図的な参加者であったことを証明する要素が含まれていなければならない。

1. 従来の現金取引の背景

従来の現金取引では、エンドユーザーは、まず銀行からの米国連邦準備ノート（紙幣）を受け、銀行はユーザーの口座の預金残高から等価的な金額を差し引く。エンドユーザーは下記の事項を含む公開鍵を使って連邦準備ノート（紙幣）の正当性を証明できる。

- a. 磁気によって吸引できる磁気インク
- b. 紙幣にすき込まれた赤と青の繊維
- c. グラビア印刷された肖像を囲む微小な印刷
- d. 米国および紙幣の表示と共に印刷された、埋め込まれたストライプ

このシステムに対する「秘密鍵」は、マネーを印刷するための未処理材料をどのように得て、どのようにマネーを実際に印刷するかの詳細である。このような情報は、政府によって保持されており、明らかにされていない。

これらの紙幣はエンドユーザーによって業者まで運ばれ、商品またはサービスと交換される。業者も紙幣の公開鍵を使って紙幣が正当なものであることを立証する。

最後に業者は紙幣を銀行へ持って行き、ここで支払機によって再び公開鍵が検査される。紙幣が正当なものであれば、紙幣の額面の値だけ業者の銀行口座の預金残高の金額が増す。

このような取引の最終結果として、エンドユーザーの銀行の預金残高が減少され、同じ金額だけ業者の銀行の預金残高が増やされ、商品またはサービスが業者からエンドユーザーへ転送され、銀行準備ノートを他の取引にすぐに再使用できる。

2. モジュールを使ったマネー取引の例

モジュール 10 を使ったマネー取引およびデジタル証明書が連邦準備ノートと異なりデジタルデータを容易にコピーし、複製できるので、多少複雑となっている。それにも拘わらず SALT および取引シーケンス番号を使用することにより、デジタル証明書の正当性を保証できる。(次の説明では、取引への各当事者は秘密に維持できる秘密鍵と自分の RSA 鍵セットを有すると仮定する。)

a. 図 6 を参照すると、サービスプロバイダ (銀行) はモジュール 10 内に記憶されたマネーの値を示すマネーオブジェクトを含む取引グループ 40 を作成することにより、モジュール 10 を作成する。サービスプロバイダは取引カウンタオブジェクト、モジュラスオブジェクトおよび指数オブジェクトも作成し、指数オブジェクトにプロバイダの秘密鍵を記憶する (D1)。サービスプロバイダは読み取りできないように鍵を秘密にする (D2)。次に、マネー取引を実行するように取引グループ 40 内に取引スクリプト 44 を記憶し、マネー取引を実行し、別のオブジェクトを作成できないように (D3) グループをブロックする (D4)。(この取引スクリプトが何を行うかの詳細については、下記で更

に説明する。)最後に、誰もが公開鍵を得ることができるようにサービスプロバイダが対応する公開鍵を公開する。

b. エンドユーザーはサービスプロバイダからモジュール10を受け、エンドユーザーの銀行口座ではモジュール10に記憶された金額が貸方に記載される。パソコンまたはハンドヘルドコンピュータを使い、エンドユーザーは預金残高が正しいかどうかを確かめるためにモジュール10に問い合わせできる。

c. 図7を参照する。エンドユーザーが業者からのある商品またはサービスを受けたい時(E1)、業者はモジュールのユニークな、レーザー食刻(lasered)登録番号を読み出し、これをランダムSALTと共にパケットに入れる(E2、E3)。次に業者は自分の秘密鍵でこのパケットにサインをし(E4)、購入金額と共に、その結果暗号化されたパケットを取引グループ40の入力データオブジェクトへ送信する(E5)。

d. 業者は次に、サービスプロバイダによってモジュール10内にプログラムされた取引スクリプト44を発動させる。この取引スクリプト44はマネーオブジェクトから購入金額を差し引き(E6)、取引カウンタオブジェクトの値を入力データオブジェクトの内容に添付し(E7)、生じたパケットに秘密鍵でサインをし、その結果を出力データオブジェクトに入れる(E8)。

e. 業者は出力データオブジェクトから結果を読み出し、これをサービスプロバイダの公開鍵で解読する(E9)。次に購入金額が正しいこと、および残りのデータが工程cでサインしたパケットに同一であることを確認する(E10)。

f. モジュール10で提供された証明書が正当かつオリジナルであること(複製でないこと)を確認した後に、業者は商品またはサービスを発送する(E11)。その後、業者はデジタル証明書を銀行へ送る。

g. 銀行はサービスプロバイダの公開鍵を用いて証明書を解読し(E12)、購入金額および取引カウントを抽出し、業者の公開鍵を使って残りのデータを解読し、モジュールのユニークな、レーザー食刻登録番号を明らかにする(E14)。銀行は次にデータベース内のユニークなレーザー食刻登録番号を使

ってモジュール10をロックアップし、この取引のための取引カウントが以前送られたものでないことを確認する。このテストに通ると、銀行はデータベースに取引カウント値を加え、次に購入金額だけ業者の銀行の預金残高を増す(E15)。証明書のこの部分がモジュール10および業者の双方によってサインされた事実により、取引が業者とモジュール10の双方が任意に同意したものであることが確認される。

取引カウンタ値、ユニークなレーザー食刻登録番号、受取人により提供されるランダムSALTおよびモジュールの秘密鍵、業者の秘密鍵またはその双方によって暗号化される購入金額のデータを組み合わせる異なる方法は多数あることに留意されたい。これら組み合わせの多くも、ユニークさ、本物であることおよび支払い拒否できないことを満足できるように保証できるものであり、ファームウェアの設計は取引スクリプト44を作成する際のサービスプロバイダのフレキシビリティによってプロバイダの特定のニーズを満たすことができる。

D. デジタル現金補充

上記I1.C章ではデジタル現金財布について説明したが、現金の補充の問題については触れていない。サービスプロバイダは別のモジュラスオブジェクトお

よびサービスプロバイダの公開鍵、ランダムSALTオブジェクトおよび預金残高にマネーを加えるための取引スクリプト44を含む指数オブジェクトを加えるだけで、I1.C章で説明したようにモジュール10に現金補充能力を加えることができる。サービスプロバイダは直に、またはネットワークを通して遠隔からモジュール10へマネーを加えることができる。このマネーを加えるプロセスは次のとおりである。

1. 図8を参照すると、サービスプロバイダはモジュールのユニークなレーザー食刻登録番号(ID番号)を読み出し(F1、F2)、ランダムSALTオブジェクトの値を戻すよう取引スクリプト44に要求する。モジュール10は先の値および乱数発生器から新しいランダムSALTの値を計算し、これをサービスプロバイダに戻す(F3)。

2. サービスプロバイダは加えるべきマネーの金額およびモジュール10

のユニークなレーザー食刻登録番号と共にモジュール10によって戻されたランダムSALTをパケットに入れ、この結果得られたパケットをサービスプロバイダの秘密鍵を用いて暗号化する(F4)。このような暗号化されたパケットは取引グループ40の入力データオブジェクト内に書き戻される。

3. サービスプロバイダの公開鍵を用いて入力データオブジェクトの内容を解読する取引スクリプト44を要求し、ユニークなレーザー食刻登録番号およびランダムSALTの値をサービスプロバイダが最初に与えたものに対してチェックする。SALTが一致していれば、パケットがマネー金額を抽出し、これをモジュール内のマネーオブジェクトの値に加える(F5)。ユニークなレーザーを使った登録番号が含まれていることは厳密には必要でないが、サービスプロバイダがファンドをどのモジュールが受けているかを正確に知ることができるようにこの登録番号が含まれていることに留意されたい。

E. モジュール間のファンドの直接送金の説明

上記II. C. 2. g章では業者がデジタル証明書を自分の銀行へ戻し、業者の口座に対する貸方に記入する際に問題が生じることを示した。業者側の銀行は払い戻しのためにサービスプロバイダに証明書を送り戻すか、または取引カウン

トオブジェクトの値がユニークであるかどうかを判断できるように、データベース内のサービスプロバイダの記録にアクセスしなければならない。このことは不便であり、これを行うためのインフラストラクチャを必要とする。また、業者側の銀行は使用済みの証明書の番号が再使用されないように、この証明書の番号をデータベースにロギングしなければならないので、このことは取引のいずれかが匿名(現金が既に使用された場合になるように)となることも防止する。これら問題は、モジュール間のファンド送金を活用することによりすべて除くことができる。更に、モジュール間のファンド送金を行うのに必要な工程は、II. C. 2章に記載されている工程よりもかなり簡単である。

次の説明では、業者もエンドユーザー(顧客)から受け取ったファンドを集めるのに使用するモジュールを有する。以下、エンドユーザーの所有するモジュールを「支払い人」と称し、業者の所有するモジュールを「受取人」と称す。ファ

ンド送金を行うための工程は次のとおりである。

1. 図9、11および12を参照する。業者は自分のコンピュータを使用して受取人内の取引スクリプト44に要求して、ランダムSALTを提供させる。業者は取引グループ40の出力オブジェクトからこのSALTを読み出す。

2. 業者はこのSALTおよびエンドユーザーの購入金額を支払い人の入力データオブジェクトにコピーし(G1)、支払い人内の取引スクリプト44に要求して、預金残高から購入金額を差し引き、パケット内の受取人のSALTと購入金額とを組み合わせ、この結果得られたパッケージをサービスプロバイダの秘密鍵で暗号化し、これを出力データオブジェクトに戻させる(G2)。

3. 次に業者はこのパケットを読み出し、これを受取人の入力データオブジェクトにコピーし、受取人内の取引スクリプト44に要求してパケットをサービスプロバイダの公開鍵で解読し(G3)、SALTを、受取人が最初に発生したものと照合する。これらが一致していれば、受取人は購入金額を預金残高に加える(G4)。

これによりファンド送金が完了する。この取引は支払い人から受取人へ購入金額を有効に転送し、取引の工程はII. C. 2に記載した3方向取引よりもかなり簡単であることに留意されたい。銀行がSALTを業者のモジュールへ送り、業者が銀行へ送った預金残高の証明書を業者のモジュールが作成する同様な取引

により、業者は自分の銀行口座へ預金残高を転送できる。ファンドを集めるために業者がモジュールを使用することにより取引が簡略になり、ユニークさを確認するためのデータベースが不要となり、通常、キャッシュ取引で生じるようなエンドユーザーの匿名性が留保できる。

F. ネットワークを通したモジュールを使った取引例

上記II. C. 2、II. DおよびII. E章に記載の取引は、ネットワークを通して行うことができ、これにより業者とエンドユーザーとモジュールとを物理的に分離できる。しかしながらこれにより、モジュール10に対する組み合わせのうちの1つが暗号化されず、よって偽造が行われ得るので、このようなネットワークを通した取引は潜在的な問題を生じ得る。この問題を回避するため、

双方の当事者は1つのSALTを発生し、他方の当事者がサービスプロバイダの秘密鍵を使ってSALTを暗号化できることを実証し、よって正当性を証明しなければならない。このような操作はモジュール間のファンドの送金（上記11. E章）に関連するように、次のように説明される。この方法は、上記取引のうちの任意のものがネットワークを通して行うことができるように使用できる。これにより、明らかにインターネットを通した安全な電子的な取引が可能となる。

1. 図10、11および12を参照する。支払い人はランダムSALTを発生し、ネットワークを通してこれを受取人に送信する（H1）。

2. 受取人は支払い人のSALTに購入金額を加え、その後に受取人によってランダムに発生されたSALTが来る。次に受取人はこのパケットをサービスプロバイダの秘密鍵で暗号化し、これを支払い人に戻す（H2）。

3. 支払い人はパケットをサービスプロバイダの公開鍵で解読し（H3）、支払い人のSALTを抽出し、これを支払い人が工程1で与えたSALTと比較する。これらが一致していれば、支払い人は預金残高から購入金額を差し引き、購入金額とサービスプロバイダの秘密鍵で暗号化した受取人のSALTからなる証明書を発生し、これを受取人へ戻す（H5）。

4. 受取人はパケットをサービスプロバイダの公開鍵で解読し（H6）、受取人のSALTを抽出し、これと、受取人が工程2で与えたSALTとを比較し、これらが一致していれば、受取人は自分の預金残高に購入金額を加える（H7）。

SALTの交換により各モジュールは他のモジュールと通信していること、よってリクエストされたファンド送金が正当なものであることを確認できる。工程3で述べたSALTの比較により、支払い人はファンドを引き出す前に受取人が正当なモジュール10であることを確認でき、工程4に記載の比較により受取人はファンドを入金する前に支払い人が正当なモジュール10であることを確認できる。上記取引により、暗号化されたパケット内の必要な最小量の情報が得られ、よってファンドが1つのモジュール10から他のモジュールに送金されていることを確認できる。付加情報を提供しそして取引をより完備するために、ユニー

クな、レーザー食刻登録番号のような他の情報を（匿名性を犠牲にして）含ませることもできる。

G. ソフトウェアの正当化および使用量の計量のための技術例

モジュール10は包括的なソフトウェアシステムにおける特定のソフトウェアの特徴を可能にするタスクおよびこれら特徴の利用を計量化するために良好に適している。（この使用モデルはモジュール10からマネーを引き出すための、これまで説明したモデルに匹敵するものである。）

1. 準備

図11および12を参照する。サービスプロバイダは取引グループ40を作成し、エンドユーザーがモジュール10内のどのソフトウェアを使用するのかが許可されるかを詳細に定めるグループ内にコンフィギュレーションオブジェクトを記憶する。更に許可された使用クレジット（これは実際のドルの金額ではなく、時間単位とすることができる）を含むマネーオブジェクトも作成し、正当化のために使用するよう、秘密RSA鍵ペアを記憶し、これを秘密にする。取引スクリプト44を記憶し、SALTおよび金額を受け取り、エンドユーザーから引き出し、引き出した金額だけ預金残高を引き下げ、引いた金額、販売およびコンフィギュレーションオブジェクトの値を含むRSAでサインされた証明書を出力する。

2. 使用

モジュール10内のソフトウェアを使用する間の周期的なインターバルで、パソコンのプログラムはランダムSALTおよびモジュール10の使用に対する料金の金額を発生し、この情報をモジュール10へ送信する。モジュール10は預金残高をデクリメントし、証明書を戻す。パソコンは証明書を解読し、SALTが同一であり、引いた金額が正しく、コンフィギュレーションオブジェクト内に記憶されている情報によりモジュール10内のソフトウェアの使用が正当化されたことを確認する。これらの検査のいずれにも成功すると、モジュール10は別の証明書がモジュール10に求められるまで、所定の時間の間、または所定の操作回数だけ実行する。

この使用モデルには多数の変形例が可能になる。例えば取引スクリプト44はパソコンで実行されるアプリケーションプログラムが実行時間を正確に測定することを保証できるよう、証明書内に真の時間をバインドすることも可能である。

(これを行うには、測定時間の基準を与えるための初期化中にサービスプロバイダがクロックオフセットオブジェクトを発生しなければならない。)

H. 取引タッチメモリ (商標) のシミュレーション

この使用モデルは、より簡単な取引タッチメモリ (商標) (DS1962年) (以下TTMとする) またはこれと均等または同様に作動できる同様なデバイスまたは置換物の作動をシミュレートするのにモジュール10をどのように使用できるかを述べるものである。TTMの基本的な特徴は、メモリブロックの内容が変更された時はいつも、カウンタを自動的にインクリメントするように、メモリブロックと連動したカウンタが設けられていることである。

1. 準備

この簡単な特徴は、コンフィギュレーションオブジェクトと、取引カウンタオブジェクトと、取引スクリプトオブジェクト (このオブジェクトは入力オブジェクトの内容と取引カウンタオブジェクトの値を組み合わせ、これらをコンフィギュレーションオブジェクトに入れる) を作成し、プロセス内でカウンタを自動的にインクリメントすることにより、モジュール10にプログラムできる。3つのすべてのオブジェクト42はロックされるが、いずれも秘密にはされない。

2. 使用

マネーを加えたり、引き出したりするのに、エンドユーザーはコンフィギュレーションオブジェクトおよび取引カウンタオブジェクトの値を直接読み出し、コ

ンフィギュレーションオブジェクトを解読し、解読されたパッケージからの取引カウンタとカウンタオブジェクトの値とを照合する。エンドユーザーは暗号化されたパケットからのユニークな、レーザー食刻登録番号とモジュール10の登録番号とを照合する。これらが一致していれば預金残高を有効と見なす。預金残高から所定の金額を加えたり、差し引きし、取引カウンタをインクリメントし、パケットを再び暗号化し、これを入力データオブジェクトに記憶する。次にデータ

および取引カウンタ値をコンフィギュレーションオブジェクトに移すのに取引スクリプト44が要求され、プロセス内で自動的にカウンタ値をインクリメントする。(コンフィギュレーションオブジェクト内の値が変更されるたびに、取引スクリプト44はカウンタオブジェクトの値がインクリメントされることを保証する。)

このような簡単な操作は、モジュール10が暗号化自体を実行する必要がないので、比較的短時間で実行できる。しかしながらTTMを用いた場合のように、エンドユーザーは次に暗号化および解読操作を実行するのに安全な計算施設を使用しなければならない。従って、このような使用はモジュールの暗号化機能に依存したものよりも低いレベルに保護される。

1. 郵便計量サービスのための技術例

この使用モデルはモジュール10を使って郵便証明書を送り出すアプリケーションを説明するものである。証明書を構成するデジタル情報は二次元のバーコードとして封筒上プリントされ、このバーコードはサービスプロバイダによって読み出され、認証できる(U. S. P. S.)。モジュール10と組み合わせられてレーザープリンタに接続された通常のパソコンで作動するコンピュータプログラムを使って郵便証明書をプリントできる。

1. 準備

サービスプロバイダはマネーレジスタ、どのモジュールにも共通な秘密RSA鍵(指数オブジェクトおよびモジュラスオブジェクト)と取引スクリプト44を含むグループを作成する。スクリプト44はSALTおよび(エンドユーザーのコンピュータによって与えられる)引出し金額とモジュール10のユニークな、レーザー食刻登録番号とを組み合わせ、このパケットを秘密鍵で暗号化し、預金

残高から金額を差し引き、出力オブジェクト内に暗号化された証明書を入れ、ここで証明書をパソコンで読み出すことができる。

サービスプロバイダは所定のマネー金額で預金残高を初期化し、預金残高およびスクリプト44をロックし、RSA鍵オブジェクトを秘密にし、それ以上スクリプトを加えることができないようにグループをロックする。このように作成さ

れたモジュールをパソコンに基づく郵便計量プログラムと共に使用できるように、カウンタを通して販売できる。

2. 使用

最初の封筒をプリントすべき際に、パソコンプログラムは日および一部のユニークなレーザーを使った登録番号の一方方向ハッシュ（例えば安全ハッシュ規格、F I B S P U B 180）を計算することにより、最初のS A L Tを作成する。この情報は、引き出すべき郵便量と共にモジュール10へ送られる。この結果生じた証明書はハッシュ発生番号（最初のハッシュに対しては1つ）、ユニークなレーザー食刻登録番号、スタンプの平文表示、日およびエンドユーザーを識別したい場合の他の情報と共に、二次元バーコードとしてプリントされる。その後のS A L Tは先のS A L Tに対し一方方向ハッシュを再び実行し、ハッシュ発生番号をインクリメントすることによって発生される。

サービスプロバイダが封筒を受けると、封筒のほとんどは額面の値が読み取られ、デジタルバーコードは読み取られない。しかしながらバーコードの統計的なサンプリングを読み取り、得られた情報を公開鍵で解読し、証明する。食い違いを調査し、現行法により偽造を追求する。サンプリングはユニークなレーザー食刻登録番号、日付およびハッシュ発生番号からS A L Tを再作成し、取引が現在のものであるだけでなく、特定のモジュール10にリンクしていることを立証できる。

同様な結果を生じさせる上記方法には、可能な変形例は多数ある。最もあり得る偽造は複製であり、これはユーザーがプリンタへ送るデジタル情報を捕捉し、郵便証明書を作成し、証明書と同じ複製コピーを多数作成する偽造である。このような偽造はハッシュ発生番号およびユニークな登録番号を読み出し、これらをデータベースでルックアップし、ユーザーが同じ証明書を複製しているかどうか

を確認するだけで、サービスプロバイダはこの複製を容易に見つけることができる。（このようなチェックはR S A解読が必要な完全な証明書の立証よりも頻繁に行うことができる。）

J. 加入情報サービス

この使用モデルは利用可能な情報に対し支払いを行うことに同意したユーザーに対し、インターネットを通して暗号化されたフォームの利用可能な情報をサービスプロバイダが作成するアプリケーションについて述べたものである。このアプリケーションは上記A章で述べた安全なEメール使用モデルと全く同じように働くが、サービスプロバイダがユーザーにEメールで送った暗号化された情報に対し、ユーザーに料金を請求する点が異なっている。この課金情報は、サービスプロバイダの公開鍵またはサービスプロバイダのモジュール10のユニークなレーザーを使ったシリアル番号に基づき、サービスプロバイダがユーザーを識別し、課金できるようにする公開RSA鍵のレジストリ(registry)から得られる。

K. 保証された秘密鍵の安全性によるレジストリ

業者にエンドユーザーの識別を別個に独立して確認させるには、サービスプロバイダはモジュール10の発行者の氏名、住所および他の識別情報と共に、特定モジュール10の公開鍵を含むレジストリを維持したいと考えることがある。この目的のために、レジストリ内の公開鍵がモジュール10にしかわからない秘密鍵に対応していることをサービスプロバイダが確実にすることが重要である。これを保証するために公開鍵がモジュール10から抽出され、レジストリに入れられる際に、モジュール10はサービスプロバイダが所有していなければならない。この情報をレジストリに記録した後、サービスプロバイダはレジストリに名前のあるエンドユーザーにモジュール10を出荷できる。

モジュール10をエンドユーザーが受け取った際に、秘密鍵がサービスプロバイダには知られず、またサービスプロバイダの被雇用者の誰にも知られていないことをエンドユーザーが確認できることも重要である。理想的なレジストリシステムはいずれかの当事者が他の当事者を信頼することを求めるべきでないで、このようなことは重要である。このシステムは各当事者が他の当事者のいずれも秘密鍵を知る可能性がないと確信できる時に限って、だれもが満足できるように働く。

これを達成するための1つの方法として、サービスプロバイダがモジュール10にコマンドを送り、乱数を使った完全なRSA鍵セットをモジュール10に発

生させ、次に、指数のうちの1つを自動的に秘密にし、よってだれもが秘密鍵の値を発見できないようにする方法がある。この鍵セットはサービスプロバイダによってカン内にプログラムされた鍵セットと異なる特殊なタイプを有し、よってモジュール10により直接ビジネスを行う者がモジュール10だけにしか秘密鍵が知られていないと、自ら判断できる。

1. 準備

サービスプロバイダはアプリケーションに対するパスワードで保護された取引グループ40を作成し、モジュール10が発生したグループ内にRSA鍵を作成する。鍵セットの発生をモジュラスおよび指数は自動的にロックされるが、第2の指数はモジュール10のファームウェアによって自動的に秘密にされる。サービスプロバイダは次に入力オブジェクトからのデータを秘密鍵で暗号化する取引スクリプト44を作成し、暗号化された結果を出力オブジェクトに入れる。この取引スクリプト44はオプションとして入力オブジェクトからのデータに別の情報（例えば取引カウンタ）を添付し、アプリケーションの別の目的を満たしてもよい。別のオブジェクト42および取引スクリプト44をサービスプロバイダの裁量で加えてもよい。取引グループ40は完全になった時にサービスプロバイダによってロックされる。次に、サービスプロバイダは取引グループ40からRSAモジュラスおよび公開指数を読み出し、これをエンドユーザーを識別する情報と共にレジストリに記録する。最後に、サービスプロバイダはモジュール10をエンドユーザーに出荷し、その後、取引グループ40にアクセスするのに使用できるパスワードをエンドユーザーに送る。

2. 使用

業者がインターネットまたは他のネットワークを通してエンドユーザーの確実な識別を得たいとき、業者はデータのユニークなパケットを発生し、これをエンドユーザーに送信し、エンドユーザーはデータを入力オブジェクトに送り、モジュール10が発生した暗号鍵で暗号化させる取引スクリプト44を要求する。こ

の結果生じた暗号化されたパケットは業者へ戻されるよう送信される。次に業者は、エンドユーザーに属す公開鍵を得るようにサービスプロバイダによって提供

されるデータベースにアクセスし、エンドユーザーの公開鍵を使って暗号化されたパケットを解読しようとする。解読に成功すれば、業者は遠隔地のネットワーク化されたロケーションでエンドユーザーのモジュール10が物理的に存在することを証明した。遠隔地におけるエンドユーザーのモジュール10が存在することを保証することにより、この識別によりデータパケットの内容、従ってエンドユーザーがリクエストできるパケットの内容によって表示される金融取引を有効にし、かつ正当化する。

ここに述べたモデルは金銭取引を実行する権限がサービスプロバイダによって維持されるレジストリから得られるモデルとなっている。従って、この情報は正確であり、モジュール10内の秘密鍵をすべての当事者から安全にできることが重要である。各モジュール10は自己のユニークなRSA鍵セットを有するので、このモデルではモジュール10がサービスプロバイダによって維持されるレジストリと独立してマネーを表示する手段はない。その代わりに、レジストリおよびモジュール10が秘密鍵と共にサインできる能力が他の当事者と離間してエンドユーザーを識別するための定義手段として働く。

L. 取引量の課税

この使用の章は、サービスプロバイダがモジュール10によって送金されるマネーの総額のあるパーセントであるサービス料金をエンドユーザーから集めようとするビジネスモデルに関する。このモデルは上記のC、D、EおよびF章に記載されたものと類似しているが、所定の日および時間に特定の取引スクリプト44を終了できるデストラクタオブジェクトが加えられている。このモデルはモジュール10から送られたすべてのマネーの総計の値を累積するように（適当な取引スクリプト44と共に）プログラムされる別のマネーオブジェクトを使用することも必要とする。

1. 準備

サービスプロバイダは上記DおよびE章に記載したように、マネーオブジェクト等を含む取引グループ40を作成する。サービスプロバイダは更に取引量累積

器として働くように別のマネーオブジェクトも作成する。このサービスプロバイ

ダはDおよびEにおけるように、マネーを引き出したり、預金するための取引スクリプト44も作成するが、モジュール10にマネーを加えるための取引スクリプトが将来の所定時間に終了するようにセットされたデストラクタオブジェクトおよびマネーを引き出すための取引スクリプト44が引出し額を取引量累積器として働くマネーオブジェクトに加えるための命令を含む点が異なる。サービスプロバイダはグループをロックし、モジュール10をエンドユーザーに出荷する。

2. 使用

エンドユーザーは上記DおよびE章に記載されているように、預金および引出しのためのモジュール10を使用する。モジュール10を使用している間、モジュール10から消費したマネーのすべての累積総量は取引量累積器として働くマネーオブジェクトに累積される。制限時間が終了すると、エンドユーザーはこのモジュール10にマネーを加えることはできないが、所望すれば何も残らなくなるまでマネーを引き出し続けることができる。次にエンドユーザーはモジュール10をサービスプロバイダへ戻し、回収される。サービスプロバイダはマネーの残高を読み出し、更に取引量累積器内に記録された金額を読み出す。サービスプロバイダは取引量累積器内の金額のパーセントであるサービス料金をエンドユーザーに請求する。エンドユーザーがこのサービスを続けるよう、この額を支払いたい場合、取引グループ40を破壊し、再構築し、エンドユーザーが戻した時のモジュール10内に残っていたマネーの残高が取引グループ40のうちのマネーオブジェクトに戻されるようにプログラムされる。エンドユーザーがサービス料金を払うことを条件に、サービスプロバイダは回収されたモジュールをエンドユーザーに戻す。

上記システムによりサービスプロバイダはエンドユーザーが行うどの金融取引もモニタしたり、またこれに加入することなくサービスに対する定期料金を集めることができる。この料金は取引量レジスタの内容によって決定される実際の使用に基づく。

モジュールと共に使用するためのファームウェアの定義例

オブジェクト

モジュールファームウェアによって取り込まれ、操作される最も原始的なデータ構造である。次の章で有効オブジェクトおよびそれらの定義のリストについて説明する。

グループ

オブジェクトの内蔵された集合である。オブジェクトの範囲はメンバーであるグループに限定される。

グループID

特定グループを表示する、好ましくは0～255の間の番号。

オブジェクトID

特定グループ内の特定のオブジェクトを表示する、好ましくは0～255の間の番号。

オブジェクトタイプ

特定オブジェクトを記述する、好ましくは1バイトタイプの特定子(specifier)。

PIN

好ましくは長さが8バイトの英数字個人識別番号

共通PIN

監査トレイルのような共用リソースへのアクセスを制御するPINである。グループを作成し、削除するホストの能力を制御することにも使用される。

グループPIN

グループ内のオブジェクトに固有の操作に対するアクセスを制御するPINである。

監査トレイル

モジュールをロックした後に生じる取引の記録

ロックされたオブジェクト

オブジェクトロックコマンドを実行することによってロックされたオブジェクトのこと。一旦オブジェクトがロックされると、これを直接読み出すことはできない。

秘密オブジェクト

オブジェクト秘密化コマンドを実行することによって秘密にされたオブジェクト。オブジェクトが一旦秘密にされると、これを直接読み出したり書き込んだりすることはできなくなる。

ロックされたグループ

グループロックコマンドを使ってロックされたグループのこと。グループが一旦ロックされると、このグループはオブジェクトを作成できなくなる。

複合オブジェクト

いくつかのオブジェクトの組み合わせ。個々のオブジェクトは複合オブジェクトの属性を受け継ぐ。

オブジェクト定義の例

R S Aモジュラス

長さが最大124ビットの大きな整数。これは、それぞれが所望するモジュールサイズの長さのビット数の約半分である2つの大きい素数の積である。このR S AモジュラスはメッセージMを符号化したり解読したりするための次の式で使われる。

$$(1) \text{暗号化: } C = M^e \pmod{N}$$

$$(2) \text{解読: } M = C^d \pmod{N}$$

ここでCは暗号文であり、dおよびeはR S A指数（下記参照）であり、NはR S Aモジュラスである。

R S A指数

（上記式1および2に示された）eおよびdの双方はR S A指数である。これらは一般に大きい数字であるが、モジュラス（N）よりも小さい。R S A指数は秘密でも公開されていてもよい。モジュールでR S A指数を作成すると、これらは公開指数または秘密指数のいずれかに宣言できる。一旦作成されると、指数は公開指数から秘密指数に変更できる。しかしながら指数が秘密にされると、指数が属する取引グループ40が破壊されるまで、この指数は秘密指数のままである。

取引スクリプト

取引スクリプトはモジュールが実行すべき一連の命令である。要求されるとモ

ジュールファームウェアはスクリプト内の命令を解釈し、その結果を出力データ

オブジェクトに入れる（下記参照）。実際のスクリプトは単なるオブジェクトのリストにすぎない。オブジェクトがリストされている順序はオブジェクトで実行すべき操作を指定する。取引スクリプト44は、好ましくは128バイトの長さとすることができる。

取引カウンタ

取引カウンタオブジェクトは長さが4バイトであることが好ましく、通常、作成時にゼロに初期化される。このオブジェクトを基準とする取引スクリプトが要求されるごとに、取引カウンタは1だけインクリメントされる。取引カウンタがロックされると、このカウンタが読み出され、取り消し不能なカウンタとなる。

マネーレジスタ

マネーレジスタオブジェクトは長さが4バイトであることが好ましく、マネーまたはその他の形態のクレジットを表示するのに使用できる。このオブジェクトが作成されると、ユーザーがこの値を不正に操作されるのを防止するようにロックしなければならない。一旦ロックされると取引スクリプトを要求することによってしかこのオブジェクトの値を変更できない。マネー取引を行う代表的な取引グループ40は、マネーレジスタからの引き出しのためのスクリプトとマネーレジスタへの預け入れのためのスクリプトを有することができる。

クロックオフセット

このオブジェクトはモジュールのリアルタイムのクロックの表示とある任意の時間（例えば1970年1月1日12:00am）との間の差を含む4バイトの数字であることが好ましい。この真の時間はクロックオフセットの値をリアルタイムクロックに加えることによりモジュールから得ることができる。

SALT

SALTオブジェクトは長さが20バイトであることが好ましく、作成時にランダムデータで初期化すべきである。ホストが発生ランダムSALTコマンドを送信すると、モジュールは好ましくは新しいランダムSALTを発生するように、先のSALTと（好ましくはランダムに生じたパワーアップによって生じた）

モジュールの乱数とを組み合わせる。SALTオブジェクトが秘密にされない場合、このオブジェクトはその後、読み出しオブジェクトコマンドを発生することによ

り読み出しできる。

コンフィギュレーションデータ

このデータは好ましくは128バイトの最大長さを有する、ユーザーが定める構造である。このオブジェクトは一般に取引グループ40に固有なコンフィギュレーション情報を記憶するのに使用される。例えば、このコンフィギュレーションデータオブジェクトを使ってマネレジスタオブジェクトのフォーマット（すなわちオブジェクトが表示する通貨のタイプ）を指定できる。このオブジェクトは予め定義された構造を有しないので、取引オブジェクトによって使用することはできない。

入力データ

入力データオブジェクトは、好ましくは128バイトの最大長さを有する入力バッファにすぎない。1つの取引グループは多数の入力オブジェクトを有することができる。コストは入力データオブジェクトを使って取引スクリプト44によって処理すべきデータを記憶する。

出力データ

この出力データオブジェクトは出力バッファとして取引スクリプトによって使用される。取引グループが作成される際に、このオブジェクトも自動的に作成される。このオブジェクトは好ましくは長さが512バイトであり、そのグループからパスワードの保護を引き継ぐ。

ランダムフィル

スクリプトインタプリタがこのタイプのオブジェクトに出会うと、カレントメッセージを自動的にパッドし、その長さを先行するモジュラスの長さよりも1ビット短くする。取引グループが作成される際に、このオブジェクトに対するハンドルも自動的に作成される。このオブジェクトは秘密オブジェクトであり、読み出しオブジェクトコマンドを使って読み出すことはできない。

ワーキングレジスタ

このオブジェクトはワーキングレジスタスペースとしてスクリプトインタプリタによって使用され、取引スクリプト内で使用できる。取引グループが作成される際に、このオブジェクトに対するハンドルも自動的に作成される。このオブ

ジェクトは秘密オブジェクトであり、読み出しオブジェクトコマンドを使って読み出しできない。

ROMデータ

このオブジェクトは取引グループが作成される際に自動的に作成される。このオブジェクトはロックされたオブジェクトであり、書き込みオブジェクトコマンドを使って変更できない。このオブジェクトは長さが8バイトであり、その内容はマイクロイン-Ａ-カン（商標）のROMデータの8倍と同じである。

好ましいモジュールファームウェアコマンドのセット共通PINセットコマンド（01H）

（モジュールへの）送信

01H、旧PIN、新PIN、PINオプションバイト

受信データ

CSB（コマンドステータスバイト）＝成功した場合は0であり、

そうでなかった場合は適当なエラーコード

出力長さ＝0

出力データ＝0

注：PINオプションバイトはビット状でもよいし、次の値のいずれかでよい

PIN_TO_ERASE 00000001b（マスター消去
に対してはPINを必要とする）

PIN_TO_CREATE 00000010b（グループ作成
に対してはPINを必要とする）

最初、モジュールは0（ゼロ）のPIN（個人識別番号）および0のオプションバイトを有する。一旦PINが設定されると、旧PINを与えるか、またはマ

スター消去によってしか変更できない。しかしながらオプションバイト内にPIN_TO_ERASEがセットされていれば、このPINは共通PINセットコマンドを用いた場合に限り変更できる。

共通PINセットコマンドに対する可能性のあるエラーコード：

ERR_BAD_COMMON_PIN (共通PINの一致なし)

ERR_BAD_PIN_LENGTH (新PIN長さ>8バイト

)

ERR_BAD_OPTION_BYTE (認識不能なオプションバイト)

この章で説明するすべてのコマンドに対し、ホストにより受信されるデータはリターンパケット状となる。リターンパケットは次の構造を有する。

コマンドステータスバイト (コマンドが成功した場合、0、そうでないエラーコード(1バイト))

出力データ長さ (コマンド出力長さ、2バイト)

出力データ (コマンド出力、上記長さ)

マスター消去コマンド(02H)

送信データ

02H、共通PIN

受信データ

コマンドが成功した場合、CSB=0で、成功しなかった場合ERR_BAD_COMMON_PINとなる。

出力長さ=0

出力データ=0

注：PINオプションのLSB(最小位ビット)がクリア(すなわちマスター消去に対しPINが不要)である場合、共通PIN値に対し0を送信する。一般に本明細書では常にPINが必要であると見なす。PINが設定されていなければ、PINとして0を送信すべきである。これは共通PINおよびグループPINにも当てはまる(下記参照)。PINが正しければ、ファームウェアはすべて

のグループ（下記参照）およびこれらグループ内のすべてのオブジェクトを削除する。共通PINおよび共通PINオプションバイトの双方を0にリセットする。

。

すべてを消去した後にモジュールはリターンパケットを送信する。CSBは既に述べたとおりである。出力データ長さおよび出力データフィールドの双方を0にセットする。

グループ作成コマンド (03H)

送信データ

03H、共通PIN、グループ名称、グループPIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

成功した場合、出力長さ=1であり、

成功しなかった場合、0であり、

成功した場合、出力データ=グループIDであり、成功しなかった場合0となる。

注：最大グループ名称の長さは16バイトであり、最大PIN長さは8バイトである。PIN_TO_CREATEビットが共通PINオプションバイト内でセットされ、送信されたPINが共通PINに一致しない場合、モジュールはOSCをERR_BAD_COMMON_PINにセットする。

グループ作成コマンドに対する可能性のあるエラーリターンコード：

ERR_BAD_COMMON_PIN (不正確な共通PIN)

ERR_BAD_NAME_LENGTH (グループ名称の長さ>16バイトの場合)

ERR_BAD_PIN_LENGTH (グループPIN長さ>8バイトの場合)

ERR_MIAC_LOCKED (モジュールはロックされている

)

ERR_INSUFFICIENT_RAM (新しいグループに対し
、メモリは充分でない)

グループPINセットコマンド (04H)

送信データ

04H、グループID、旧GPIN、新GPIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

出力長さ=0

出力データ=0

注：グループPINはコマンドパケット内で送信されたグループIDにより指

定されたグループ内のオブジェクトへのアクセスを限定するだけである。

セットグループPINコマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (グループのPINは一致しない)

ERR_BAD_PIN_LENGTH (新グループPIN長さ>8
バイト)

オブジェクト作成コマンド (05H)

送信データ

05H、グループID、グループPIN、オブジェクトタイプ、オブジェクト属性、オブジェクトデータ

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

成功した場合、出力長さ=1であり、

成功しなかった場合、0であり、

成功した場合、出力データ=オブジェクトIDであり、成功しなかった場合では0となる。

注：オブジェクト作成コマンドが成功した場合、モジュールファームウェアはグループIDによって指定されたグループ内のオブジェクトIDを返す。ホストによって供給されるPINが不正確であるか、またはグループがグループロックコマンドによってロックされている場合（下記記載）、モジュールはCSB内のエラーコードを返す。何らかの理由からオブジェクトが無効の場合、オブジェクトの作成もできない。例えば作成中のオブジェクトがRSAモジュラス（タイプ0）であり、長さが1024ビットより大きい場合。すべての取引スクリプトの規則に従う場合、取引スクリプトの作成に成功する。

オブジェクト作成コマンドに対する可能性のあるエラーリターンコード：

ERR_BAD_GROUP_PIN （不正確なグループPIN）

ERR_GROUP_LOCKED （グループは既にロックされている）

ERR_MIAC_LOCKED （モジュールはロックされている）

ERR_INVALID_TYPE （指定されたオブジェクトタイプは無効である）

ERR_BAD_SIZE （オブジェクト長は無効である）

ERR_INSUFFICIENT_RAM （新しいオブジェクトに対し、メモリは充分でない）

オブジェクトタイプ：RSAモジュール	0
RSA指数	1
マネーレジスタ	2
取引カウンタ	3
取引スクリプト	4
クロックオフセット	5
ランダムSALT	6
コンフィギュレーションオブジェクト	7
入力データオブジェクト	8

出力データオブジェクト 9

オブジェクト属性: ロックされた状態 00000001b

秘密にされた状態 00000010b

下記のオブジェクトロックコマンドおよびオブジェクト秘密化コマンドを使用することにより、作成後にオブジェクトをロックし、秘密にすることもできる。

オブジェクトロックコマンド (06H)

送信データ

06H、グループID、グループPIN、オブジェクトID

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

出力長さ=0

出力データ=0

注: グループID、グループPINおよびオブジェクトIDのすべてが正しい場合、モジュールは指定されたオブジェクトをロックする。オブジェクトをロックすることは取り消し不能な操作である。

オブジェクトロックコマンドに対する可能性のあるエラーリターンコード:

ERR_BAD_GROUP_PIN (不正なグループPIN)

ERR_GROUP_LOCKED (グループは既にロックされている)

ERR_MIAC_LOCKED (モジュールはロックされている)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_ID (指定されたオブジェクトは存在しない)

オブジェクト秘密化コマンド (07H)

送信データ

07H、グループID、グループPIN、オブジェクトID

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合では
適当なエラーコードとなる。

注：グループID、グループPIN、オブジェクトIDが有効な場合、オブジェクトは秘密にされる。秘密にされたオブジェクトはロックされたオブジェクトのすべての性質を共用するが、読み取りできない。秘密にされたオブジェクトは取引スクリプトによってしか変更できない。秘密にされたオブジェクトをロックすることは適法であるが、オブジェクトの秘密化はオブジェクトのロッキングよりも強力な操作であるので、このことには意味がない。オブジェクトを秘密化することは取り消し不能な操作である。

オブジェクト秘密化コマンドに対する可能性のあるエラーリターンコード：

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_GROUP_LOCKED (グループは既にロックされてい

る)

ERR_MIAC_LOCKED (モジュールはロックされている

)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

い)

ERR_BAD_OBJECT_ID (指定されたオブジェクトは

存在しない)

オブジェクトを破壊可能にするコマンド (08H)

送信データ

08H、グループID、グループPIN、オブジェクトID

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合では
適当なエラーコードとなる。

注：グループID、グループPIN、オブジェクトIDが有効な場合、オブジ

ェクトは破壊可能にされる。オブジェクトが破壊可能にされると、グループデスクトラクタがアクティブになった後にはこのオブジェクトは取引スクリプトによって使用不能となる。取引グループ内に破壊オブジェクトが操作しない場合、破壊可能なオブジェクトの属性ビットは影響がない。オブジェクトを破壊可能にすることは取り消し不能な操作である。

オブジェクトを破壊可能にするコマンドに対する可能性のあるエラーリターンコード：

ERR_BAD_GROUP_PIN (不正確なグループPIN)
 ERR_GROUP_LOCKED (グループは既にロックされている)
 ERR_MIAC_LOCKED (モジュールはロックされている)
 ERR_BAD_GROUP_ID (指定されたグループは存在しない)
 ERR_BAD_OBJECT_ID (指定されたオブジェクトは存在しない)

モジュールロックコマンド (09H)

送信データ

09H、共通PIN

受信データ

コマンドが成功すればCSB=0であり、成功しなかった場合、適当なエラーコード

成功した場合、出力長さ=2であり、そうでなかった場合、0

成功した場合、出力データ=監査トレイルサイズであり、そうでない場合、0である。

注：ホストの供給した共通PINが正しく、モジュールが先にロックされている場合、コマンドは成功する。モジュールがロックされていると、モジュールは新しいグループまたはオブジェクトを受け入れない。このことは、すべてのグル

ープが自動的にロックされることを意味する。システムまたはグループによって使用されないRAMは監査トレイルのために使用される。モジュールが成功裏にロックされるまで、監査トレイルはない。

監査トレイルの記録は6バイト長さであり、次の構造を有する。

グループID | オブジェクトID | 日/時間スタンプ

一旦監査トレイルが設定されると、取引スクリプトが実行される毎に、利用可能なサイズのバイトの第1ロケーション内に、上に示されたフォームの記録が記憶される。ここで、監査トレイルが開始する前にモジュールはロックされなければならないので、グループIDもオブジェクトIDも変更を受けないことに留意されたい。これにより常に監査トレイルを処理するアプリケーションは実行された取引スクリプトをユニークに識別できる。監査トレイルが利用可能なメモリのすべてを一旦消費すると、監査トレイルは最も古い取引記録の上に新しい取引記録を記憶する。

モジュールロックコマンドに対する可能性のあるエラーコード：

ERR_BAD_COMMON_PIN (供給される共通PINは不正確)

ERR_MIAC_LOCKED (モジュールは既にロックされている)

グループロックコマンド (0AH)

送信データ

0AH、グループID、グループPIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合、適当なエラーコードとなる。

出力長さ=0

出力データ=0

注：提供されるグループPINが正しい場合、モジュールBIOSは特定されたグループ内に更にオブジェクトが作成されるのを許可しない。グループは完全内

蔵エンティティであるので、(後述する)グループ削除コマンドを実行することにより、これらを削除してもよい。

ロックグループコマンドに対する可能性のあるエラーリターンコード:

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_GROUP_LOCKED (グループは既にロックされている)

ERR_MIAC_LOCKED (モジュールはロックされている)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_ID (指定されたオブジェクトは存在しない)

取引スクリプト要求コマンド(OBH)

送信データ

OBH、グループID、グループPIN、オブジェクトID

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合には適当なエラーコードとなる。

成功した場合、出力長さ=1であり、そうでない場合0

出力データ=予想される完了時間

注:モジュールによって戻された予想時間は16分の1秒である。CSB内にエラーコードが戻されると、予想時間は0となる。

取引スクリプト実行コマンドに対する可能性のあるエラーリターンコード:

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_ID (指定されたオブジェクトは存在しない)

オブジェクト読み出しコマンド (OCH)

送信データ

OCH、グループID、グループPIN、オブジェクトID

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

成功した場合、出力長さ=オブジェクト長さであり、そうでない場合0

成功した場合、出力データ=オブジェクトデータであり、そうでない場合、0

注：グループID、グループPINおよびオブジェクトIDが正しければ、モジュールは指定されたオブジェクトの属性バイトをチェックする。オブジェクトが秘密化されていないければ、モジュールはオブジェクトデータをホストに送信する。グループPINが無効か、オブジェクトが秘密化されていないければ、モジュールは出力長さ内の0およびリターンパケットのデータフィールドを戻す。

オブジェクト読み出しコマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_ID (指定されたオブジェクトは存在しない)

ERR_OBJECT_PRIVATIZED (オブジェクトは秘密化されている)

オブジェクト書き込みコマンド (ODH)

送信データ

ODH、グループID、グループPIN、オブジェクトID、オブジェクトサイズ、オブジェクトデータ

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合では

適当なエラーコードとなる。

出力長さ=0

出力データ=0

注：グループID、グループPINおよびオブジェクトIDのすべてが正しい場合、モジュールは指定されたオブジェクトの属性バイトをチェックする。オブジェクトがロックされているか、秘密にされている場合、モジュールはオブジェクトの先のサイズおよびデータをクリアし、これを新しいオブジェクトデータを取り替える。オブジェクトのタイプおよび属性バイトは影響されないことに留意。

オブジェクト書き込みコマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_ID (オブジェクトはグループ内に存在していなかった)

ERR_BAD_OBJECT_SIZE (指定された違法なオブジェクトサイズ)

ERR_OBJECT_LOCKED (オブジェクトはロックされている)

ERR_OBJECT_PRIVATIZED (オブジェクトは秘密化されている)

グループ名称読み出しコマンド (0EH)

送信データ

0EH、グループID

受信データ

CSB=0

出力長さ=グループ名称の長さ

出力データ=グループ名称

注：グループ名称は最大16バイト出あり、グループ名称内ですべてのバイト値は適法である。

グループ削除コマンド (0FH)

送信データ

0DH、グループID、グループPIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合、適当なエラーコードとなる。

出力長さ=0

出力データ=0

注：グループPINおよびオブジェクトIDが正しい場合、モジュールは指定されたグループを削除する。グループの削除によりグループ内のすべてのオブジェクトが自動的に削除される。モジュールがすでにロックされている場合、グループ削除コマンドは成功しない。

グループ削除コマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (不正確なグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在していない)

ERR_MIAC_LOCKED (モジュールはロックされている)

コマンドステータス情報入手コマンド (10H)

送信データ

10H

受信データ

CSB=0

出力長さ=6

出力データ=モジュールステータス構造 (下記参照)

注：この操作はPINを必要をせず、決して失敗しない。ステータス構造はつ

ぎのように定義される。

最後に実行されたコマンド (1 バイト)

最終コマンドステータス (1 バイト)

受信した時間コマンド (4 バイト)

モジュールコンフィギュレーション情報入手コマンド (11H)

送信データ

11H

受信データ

CSB=0

出力長さ=4

出力データ=モジュールコンフィギュレーション構造

注：この操作はPINを必要をせず、決して失敗しない。ステータス構造はつ

ぎのように定義される。

グループ数 (1 バイト)

フラグバイト (下記参照) (1 バイト)

監査トレイルサイズ/自由RAM (2 バイト)

このフラグのタイプはビット状であるか、つぎの値のいずれかである。

00000001b (モジュールはロックされている)

00000010b (アクセスに必要な共通PIN)

監査トレイル情報読み出しコマンド (12H)

送信データ

12H、共通PIN

受信データ

コマンドが成功した場合、CSB=0であり、そうでない場合、適当なエラーコードとなる。

成功した場合、出力長さ=新しい記録の#×6、そうでない場合、0

出力データ=新しい監査トレイル記録

注：送信された共通PINが有効であり、モジュールがロックされている場合

、新しいすべての取引記録はホストに転送される。

監査トレイル情報読み出しコマンドに対する可能性のあるエラーコード

ERR_BAD_COMMON_PIN (共通PINは正しくない)

ERR_MIAC_NOT_LOCKED (モジュールはロックされていない)

監査トレイル読み出しコマンド (13H)

送信データ

13H、共通PIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適切なエラーコードとなる。

成功した場合、新しい記録の数×6で、そうでない場合、0

出力データ=新しい監査トレイルの記録

注：送信されたPINが有効でモジュールがロックされている場合、PINは新しい取引の記録のすべてをホストへ転送する。

監査トレイル読み出しコマンドに対する可能性のあるエラーコード：

ERR_BAD_COMMON_PIN (共通PINは不正確)

ERR_MIAC_NOT_LOCKED (モジュールはロックされていない)

グループ監査トレイル読み出しコマンド (14H)

送信データ

14H、グループID、グループPIN

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適切なエラーコードとなる。

成功した場合、出力長さ=グループに対する記録の数×6で、そうでない場合、0

出力データ=グループに対する監査トレイルの記録

注：このコマンドは監査トレイル読み出しコマンドと同じであるが、送信データ内で特定されたグループIDに関連した記録しかホストに戻されないことが異なっている。これにより、他のグループの記録を見ることなく取引グループが自己の活動を記録しトラックできる。

グループ監査トレイル読み出しコマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_ID (グループIDは存在せず)

ERR_BAD_GROUP_PIN (共通PINは正しくない)

ERR_MIAC_NOT_LOCKED (モジュールはロックされていない)

リアルタイムクロック読み出しコマンド (15H)

送信データ

15H、共通PIN

受信データ

共通PINが一致する場合、CSB=0であり、そうでない場合ERR_BAD_COMMON_PINとなる。

出力長さ=4

出力データ=リアルタイムクロックの最大4つの位のバイト

注：この値はクロックオフセットでは調節されない。このコマンドは取引グループ作成中にクロックオフセットを計算するようサービスプロバイダによって通常使用される。

調節されたリアルタイムクロック読み出しコマンド (16H)

送信データ

16H、グループID、グループPIN、オフセットオブジェクトのI

D

受信データ

コマンドが成功した場合、CSB=0であり、成功しなかった場合適当なエラーコードとなる。

成功した場合、出力長さ=4、そうでない場合、0

出力データ=リアルタイムクロック+クロックオフセットID

注：グループID及びグループPINが有効であり、オブジェクトIDがクロックオフセットのIDである場合、このコマンドは成功する。このモジュールはRTCの最大位の4バイトの現在の値にクロックオフセットを加える。同じタスクを実行し、その結果を出力データオブジェクトに入れるよう取引スクリプトを書き込むことができることに留意のこと。

調節されたリアルタイムクロック読み出しコマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (正確でないグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_OBJECT_TYPE (オブジェクトIDはクロックオフセットでない)

ランダムデータを得るコマンド (17H)

送信データ

17H、長さ(L)

受信データ

コマンドが成功した場合、CSB=0であり、そうでない場合エラーコード。

成功した場合、出力長さ=L、そうでない場合は0

成功した場合、出力データ=ランダムデータのLバイト

注：このコマンドは暗号学的に有効な乱数の良好なソースとなる。

ランダムデータを得るコマンドの可能性のあるコード

ERR_BAD_SIZE (リクエストされたバイト数>128)

ファームウェアのバージョンIDを得るコマンド (18H)

送信データ

18H

受信データ

C S B = 0

出力長さ=ファームウェアのバージョンIDのストリングの長さ

出力データ=ファームウェアのバージョンIDのストリング

注：このコマンドはパスカルタイプのストリング（長さ+データ）としてファームウェアバージョンIDを戻す。

フリーRAMを得るコマンド（19H）

送信データ

19H

受信データ

C S B = 0

出力長さ= 2

出力データ=フリーRAMの量を含む2バイト値

注：モジュールがロックされている場合、出力データバイトはいずれも0となり、取引グループによって使用されないすべてのメモリが監査トレイルに対して留保されていることを示す。

グループ名称変更コマンド（1AH）

送信データ

1AH、グループID、グループPIN、新しいグループ名称

受信データ

コマンドが成功した場合、C S B = 0、そうでない場合、適当なエラーコード

出力長さ= 0

出力データ= 0

注：指定されたグループIDがモジュール内に存在し、供給されたPINが正しい場合、取引グループ名称はホストによって供給された新しいグループ名称と置き換えられる。0のグループIDが供給される場合、送信されるPINは共通PINでなければならない。正しい場合、モジュール名はホストによって供給される新しい名称と置換される。

グループ名称変更コマンドに対する可能性のあるエラーコード：

ERR_BAD_GROUP_PIN (正確でないグループPIN)

ERR_BAD_GROUP_ID (指定されたグループは存在しない)

ERR_BAD_NAME_LENGTH (新しいグループ名称>16バイト)

エラーコードの定義

ERR_BAD_COMMAND (80H)

このエラーコードはモジュールファームウェアがホストの送信した直後のコマンドを認識しない時に発生する。

ERR_BAD_COMMON_PIN (81H)

このエラーコードはコマンドが共通PINを求め、供給されたPINがモジュールの共通PINに一致しない時に戻される。最初、この共通PINは0にセットされる。

ERR_BAD_GROUP_PIN (82H)

取引グループは自己のPINを有することができる(図11)。このPINが(グループPINセットコマンドによって)セットされている場合、このPINはグループ内のオブジェクトのいずれかにアクセスするように供給されなければならない。供給されたグループPINが実際のグループPINに一致しない場合、モジュールはERR_BAD_GROUP_PINエラーコードを戻す。

ERR_BAD_PIN_LENGTH (83H)

PIN値を変更できるコマンドは2つある。すなわちグループPINセットコマンドと、共通PINセットコマンドである。これらの双方は新しいPINだけでなく旧PINも必要とする。供給された旧PINが正しいが、新PINの長さが8キャラクタよりも長い場合、このERR_BAD_PIN_LENGTHエラーコードは戻される。

ERR_BAD_OPTION_BYTE (84H)

このオプションバイトは共通PINにしか使用されない。共通PINセットコマンドが実行されるとホストが供給する最終バイトは(コマンドの章に記載した)オプションバイトとなる。このバイトがモジュールに認識不能である場合、

このバイトはERR_BAD_OPTION_BYTEエラーコードを戻す。

ERR_BAD_NAME_LENGTH (85H)

取引グループ作成コマンドが実行されると、ホストによって供給されるデータ構造の1つはグループ名称となる。このグループ名称は長さが16キャラクタを越えることはできない。供給される名称が16キャラクタよりも長い場合、ERR_BAD_NAME_LENGTHエラーコードが戻される。

ERR_INSUFFICIENT_RAM (86H)

モジュール内で利用できる十分な量がない場合、取引グループ作成コマンドおよびオブジェクト作成コマンドはこのエラーコードを戻す。

ERR_MIAC_LOCKED (87H)

モジュールがロックされていると、どのグループも、またはオブジェクトも作成したり破壊したりすることはできない。オブジェクトを作成または削除する試みにより、ERR_MIAC_LOCKEDエラーコードが発生される。

ERR_MIAC_NOT_LOCKED (88H)

モジュールがロックされていない場合、監査トレイルはない。監査トレイルコマンドのうちの1つが実行される場合、このエラーコードは戻される。

ERR_GROUP_LOCKED (89H)

一旦取引グループがロックされると、そのグループ内でのオブジェクトの作成は不可能となる。オブジェクトの属性およびタイプも凍結される。オブジェクトを作成したり、それら属性またはバイトのタイプを変更する試みがあれば、ERR_GROUP_LOCKEDエラーコードが発生される。

ERR_BAD_OBJECT_TYPE (8AH)

ホストがオブジェクト作成コマンドをモジュールに送ると、コマンドが供給するパラメータのうちの1つはオブジェクトタイプとなる（コマンドの章参照）。オブジェクトタイプがファームウェアによって認識されない場合、このオブジェクトはERR_BAD_OBJECT_TYPEエラーコードを戻す。

ERR_BAD_OBJECT_ATTR (8BH)

ホストがオブジェクト作成コマンドをモジュールに送ると、このコマンドが供給するパラメータのうちの1つはオブジェクト属性バイトとなる（コマンドの章

参照)。オブジェクト属性バイトがファームウェアによって認識されない場合、このコマンドはERR_BAD_OBJECT_ATTRエラーコードを戻す。

ERR_BAD_SIZE (8CH)

オブジェクトを作成または書き込む際に、通常、ERR_BAD_SIZEエラーコードが発生される。ホストによって供給されるオブジェクトデータが無効長さを有する場合に限り、このことが生じる。

ERR_BAD_GROUP_ID (8DH)

取引グループレベルで作動するすべてのコマンドは、グループIDがコマンドパケットで供給されることを求める。指定されたグループIDがモジュール内に存在しない場合、このIDはERR_BAD_GROUP_IDエラーコードが発生する。

ERR_BAD_OBJECT_ID (8EH)

オブジェクトレベルで作動するすべてのコマンドはオブジェクトIDがコマンドパケットで供給されることを求める。指定されたオブジェクトIDが特定の取引グループ（これもコマンドパケット内で指定される）内に存在しない場合、このモジュールはERR_BAD_OBJECT_IDエラーコードを発生する。

ERR_INSUFFICIENT_FUNDS (8FH)

金融取引を行うスクリプトオブジェクトが要求され、マネーレジスタの値が求められた引き出し額よりも少ない場合、ERR_INSUFFICIENT_FUNDSエラーコードが戻される。

ERR_OBJECT_LOCKED (90H)

ロックされたオブジェクトが読み出されるだけである。オブジェクト書き込みコマンドが試みられ、このコマンドがロックされたオブジェクトのオブジェクトIDを指定する場合、モジュールはERR_OBJECT_LOCKEDエラーコードを戻す。

ERR_OBJECT_PRIVATE (91H)

秘密オブジェクトは直接読み出しできないし、書き込みもできない。オブジェクト読み出しコマンドまたはオブジェクト書き込みコマンドが試みられ、コマンドが秘密オブジェクトのオブジェクトIDを指定すると、コマンドはERR_O

BJECT__PRIVATEエラーコードを戻す。

ERR__OBJECT__DESTRUCTED (92H)

オブジェクトが破壊可能であり、取引グループのデストラクタがアクティブである場合、スクリプトによりオブジェクトは使用できない。破壊されたオブジェクトを使用するスクリプトが要求された場合、モジュールによりERR__OBJECT__DESTRUCTEDエラーコードが戻される。

本発明の実施例は耐久性のあるステンレススチール製のトークン状の缶に入れることが好ましい。モジュールは実質的に連結可能な物品内に入れることができると解される。連結可能な物品の例としては、クレジットカード、リング、腕時計、がま口、財布、ネックレス、宝石、IDバッジ、ペン、クリップボード等がある。

モジュールは単一チップの、信頼されたコンピュータとすることが好ましい。「信頼された」なる用語は、このコンピュータが好ましくない手段によって不正な扱いから極めて安全であることを意味する。このモジュールは数学的に集中される暗号化を行うよう最適にされた数値コプロセッサを含む。BIOSは変更に対して耐力があり、極めて安全な取引ができるように特別に設計されていることが好ましい。

各モジュールは秘密鍵／公開鍵セットを作成する能力を備えた乱数シード発生器を有することができる。秘密鍵はモジュールから決して離れることなく、モジュールにしか知られていない。更に秘密鍵の発見はモジュールへの不正な侵入に対してアクティブな自動破壊作用によって防止される。このモジュールは個人の識別番号(PIN)によってユーザーに対して拘束できる。

取引がモジュールによって実行されると、モジュールおよびモジュールが通信するシステムのいずれかまたは双方によって正当化の証明書が作成される。特にこの証明書は下記を含むことができる。

- 1) ユニークな登録番号により、モジュールユーザーであるのは誰か。
- 2) 取引の真の時間スタンプにより、取引がいつ行われたか。
- 3) 登録されたモジュールインターフェースのサイトの識別により、どこで取引が行われたか。

4) ユニークに連続にされた取引およびメッセージダイジェスト上のデジタル署名による安全情報。

5) 有効、紛失または終了のように表示されたモジュールステータス。

以上で、本発明の方法および装置の好ましい実施例について添付図面に示し、これまでの詳細な説明に述べたが、本発明は開示した実施例のみに限定されるものでなく、次の請求の範囲に記載した発明の範囲から逸脱することなく、多数の再配置、変更および置換が可能であると理解できよう。

【図1】

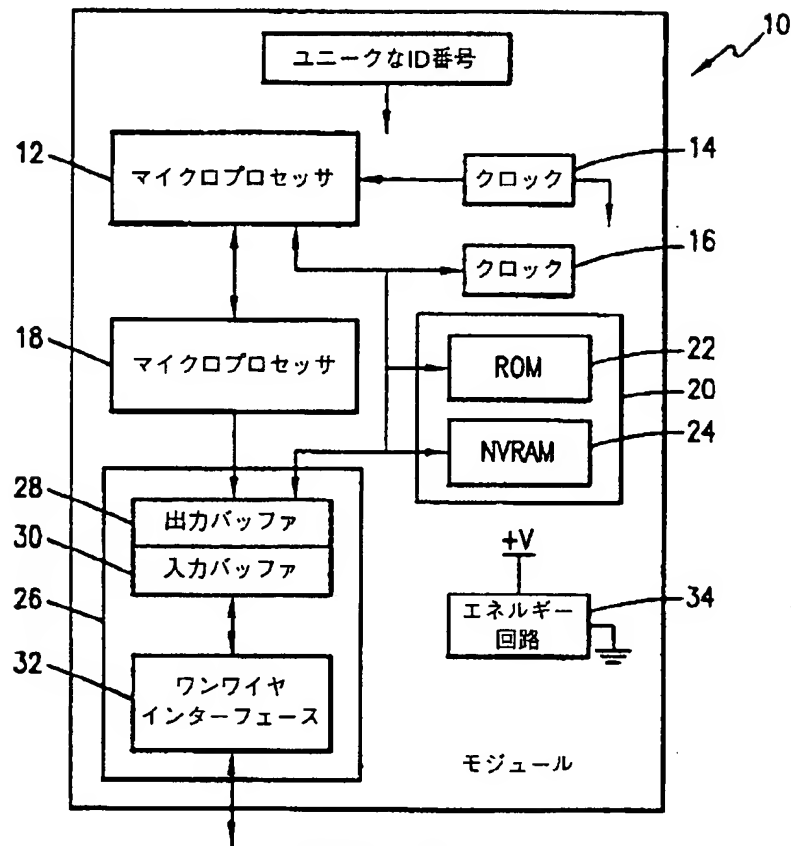
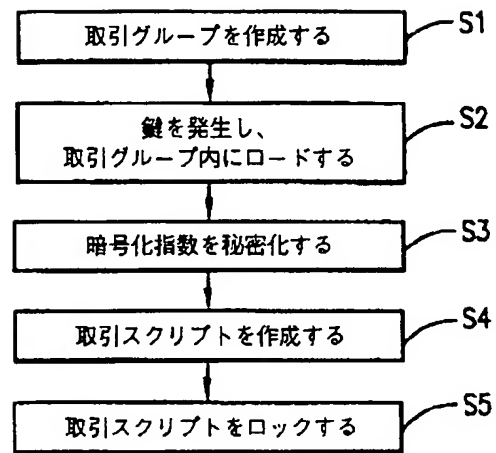
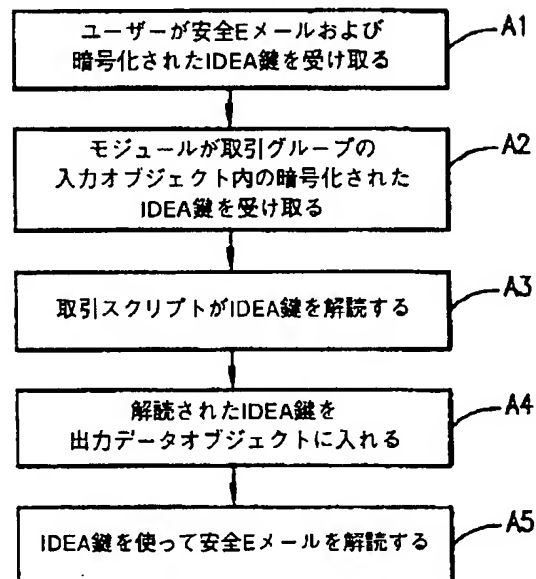


FIG. 1

【図2】

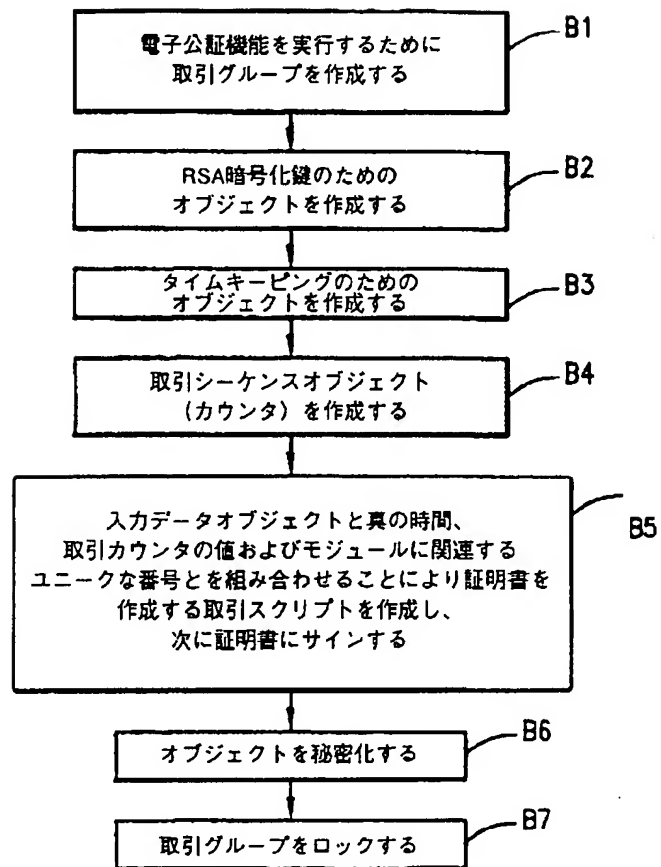
**FIG. 2**

【図3】

FIG. 3

【図4】

FIG. 4



【図5】

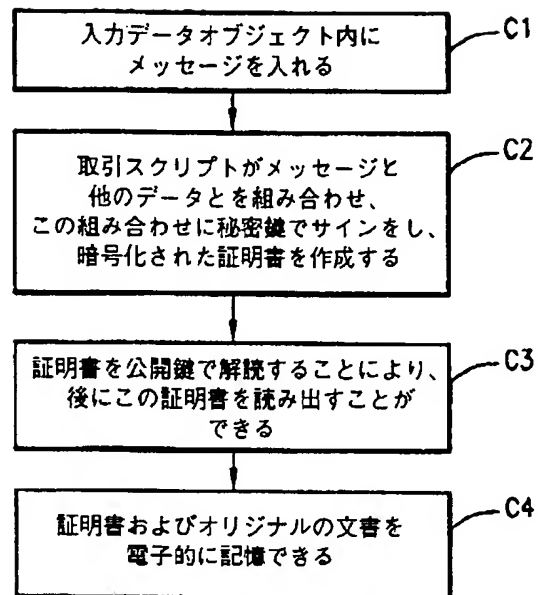


FIG. 5

【図6】

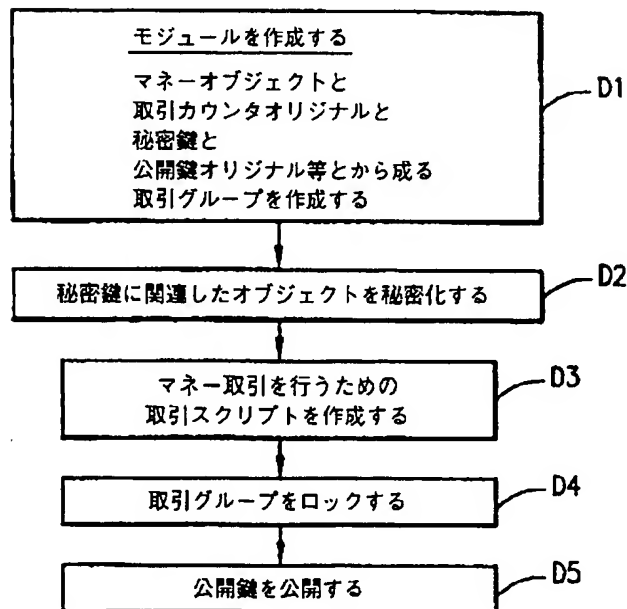


FIG. 6

【図7】

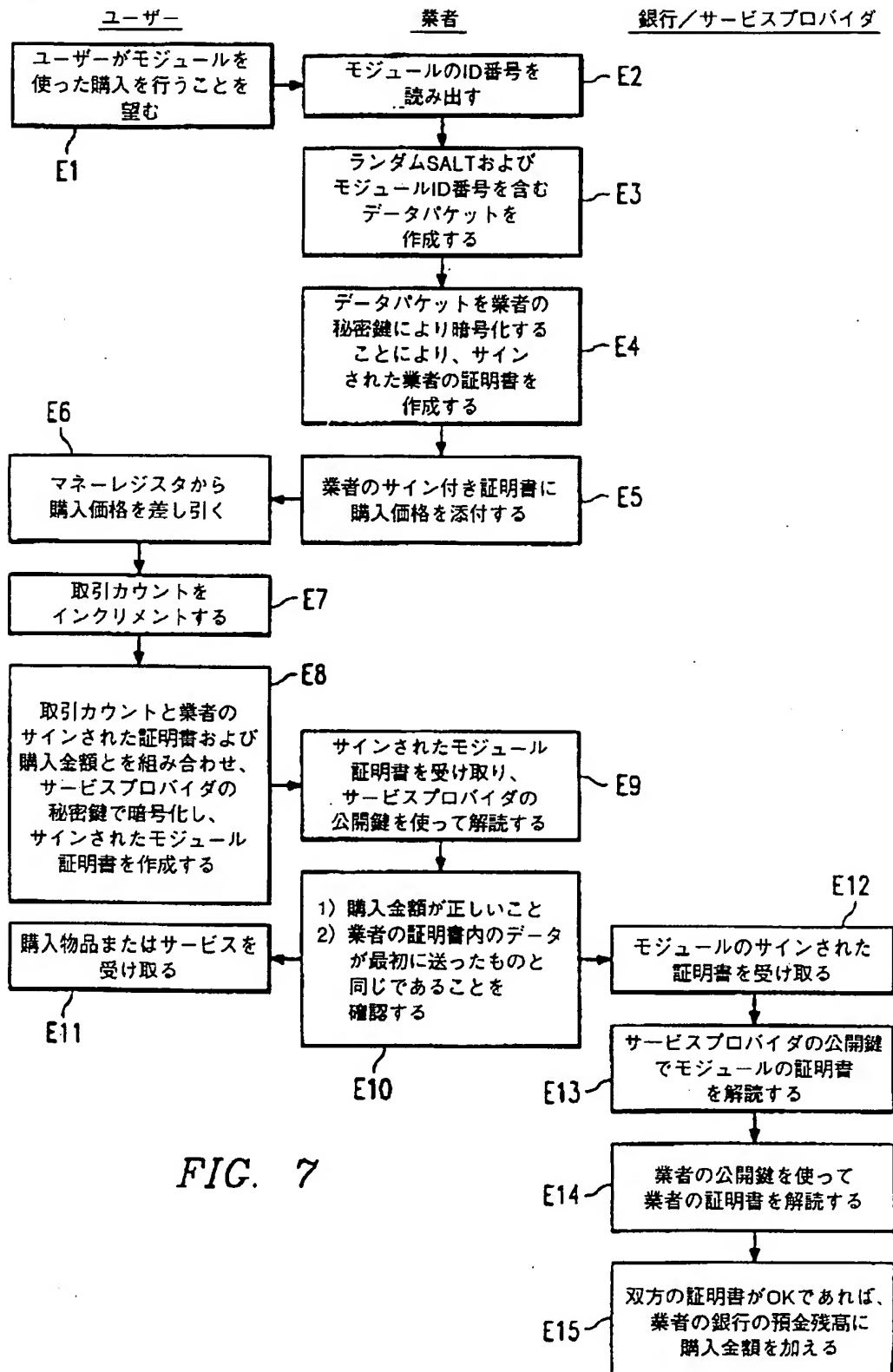


FIG. 7

【図8】

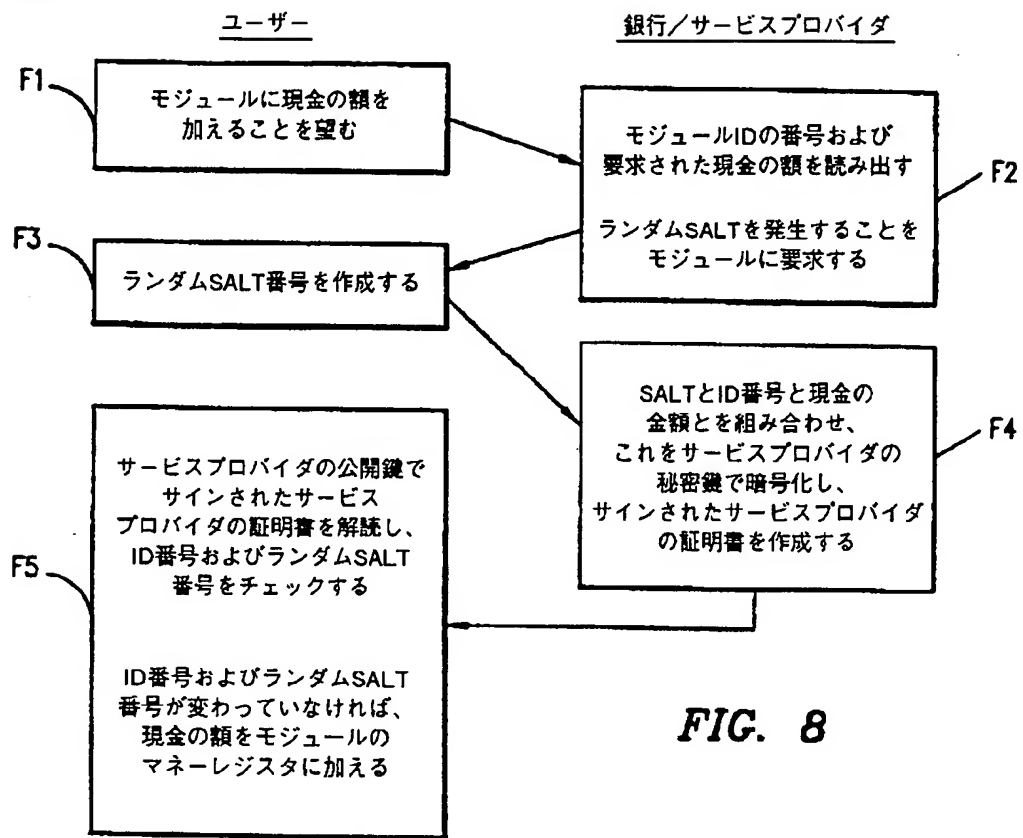
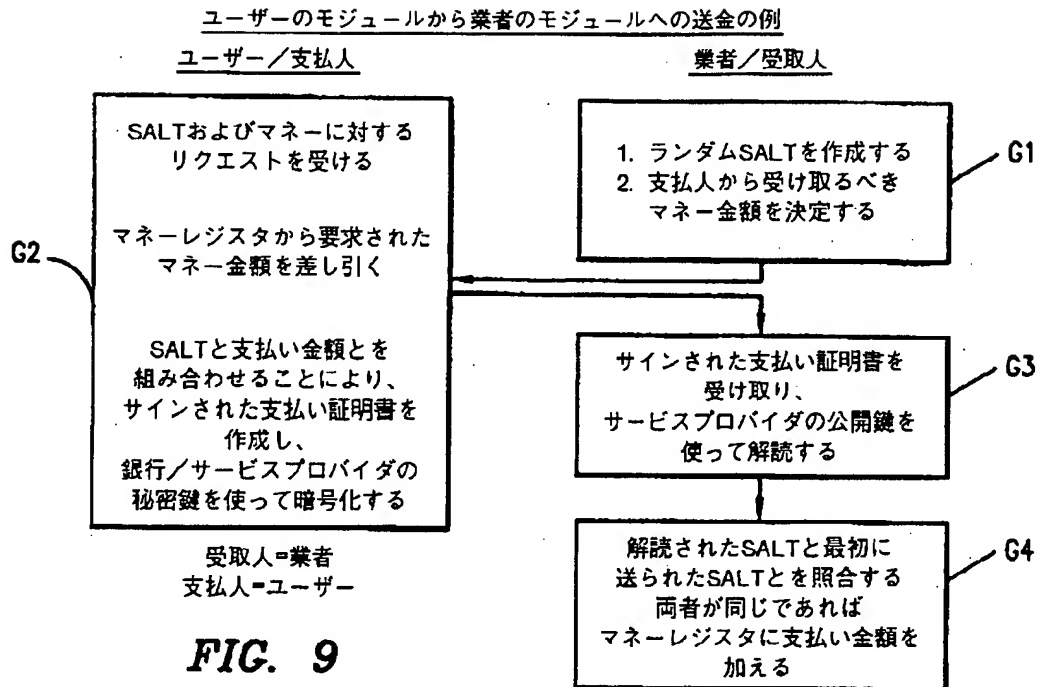


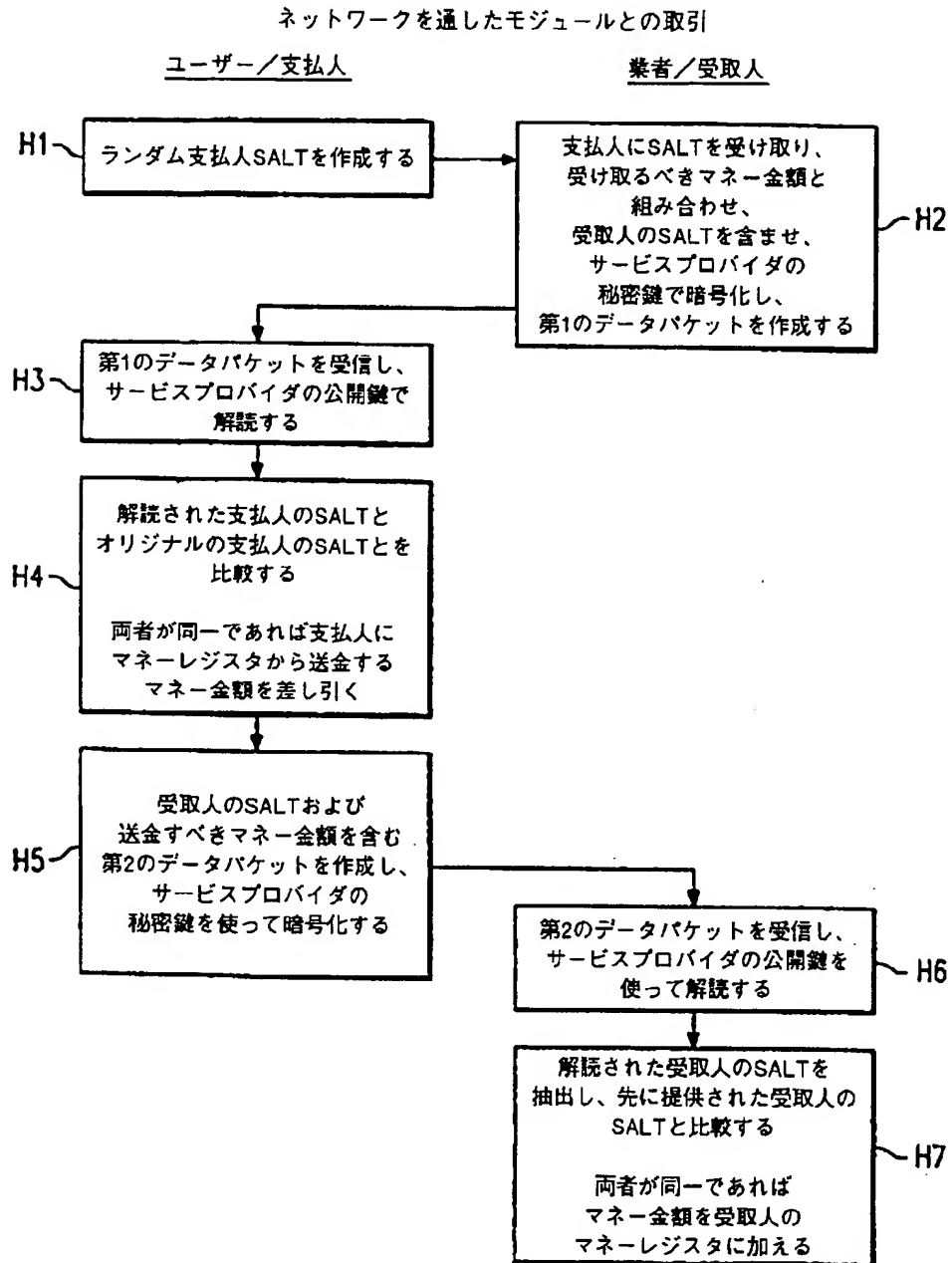
FIG. 8

【図9】



【図10】

FIG. 10



【図11】

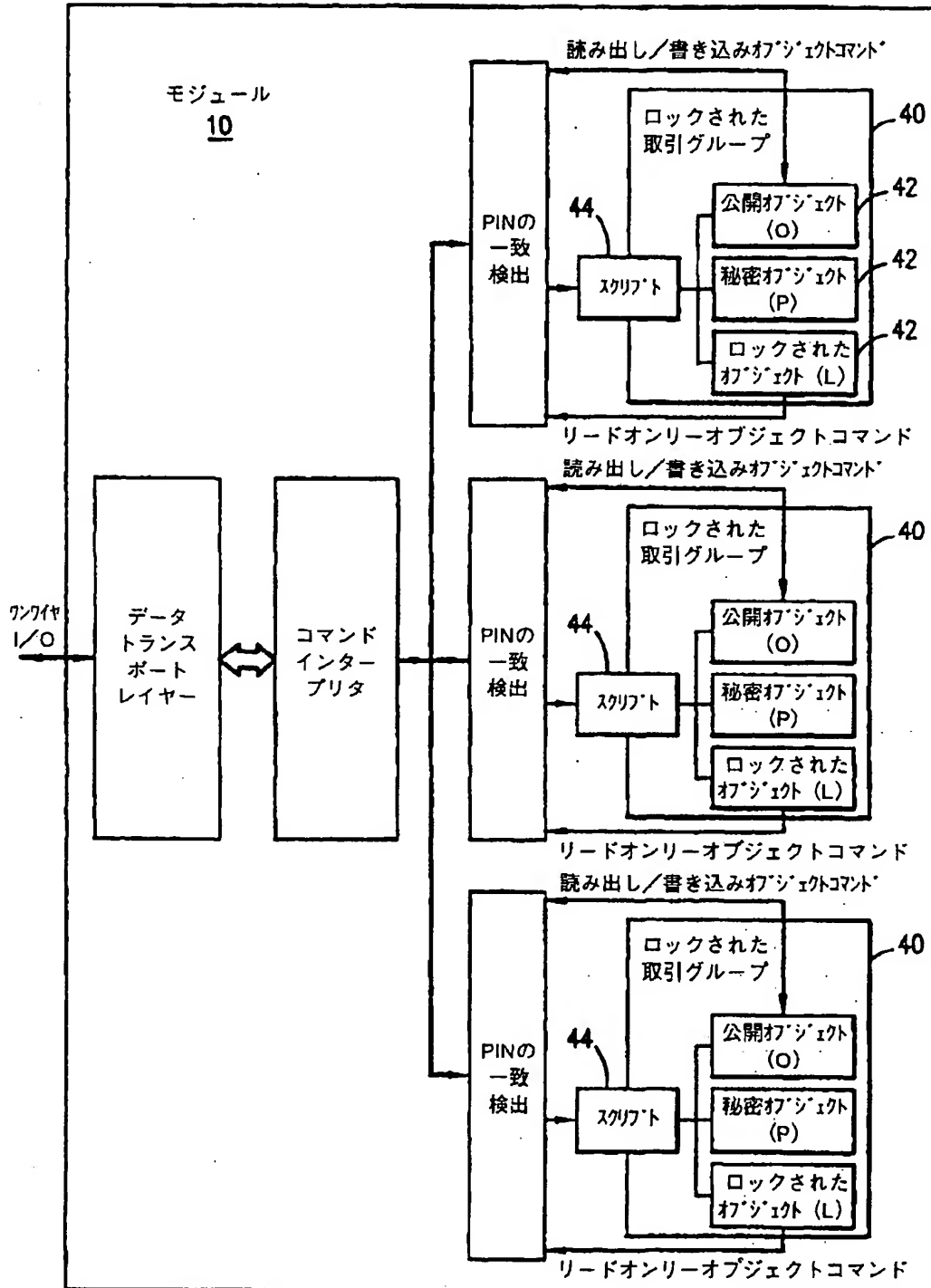


FIG. 11

【図12】

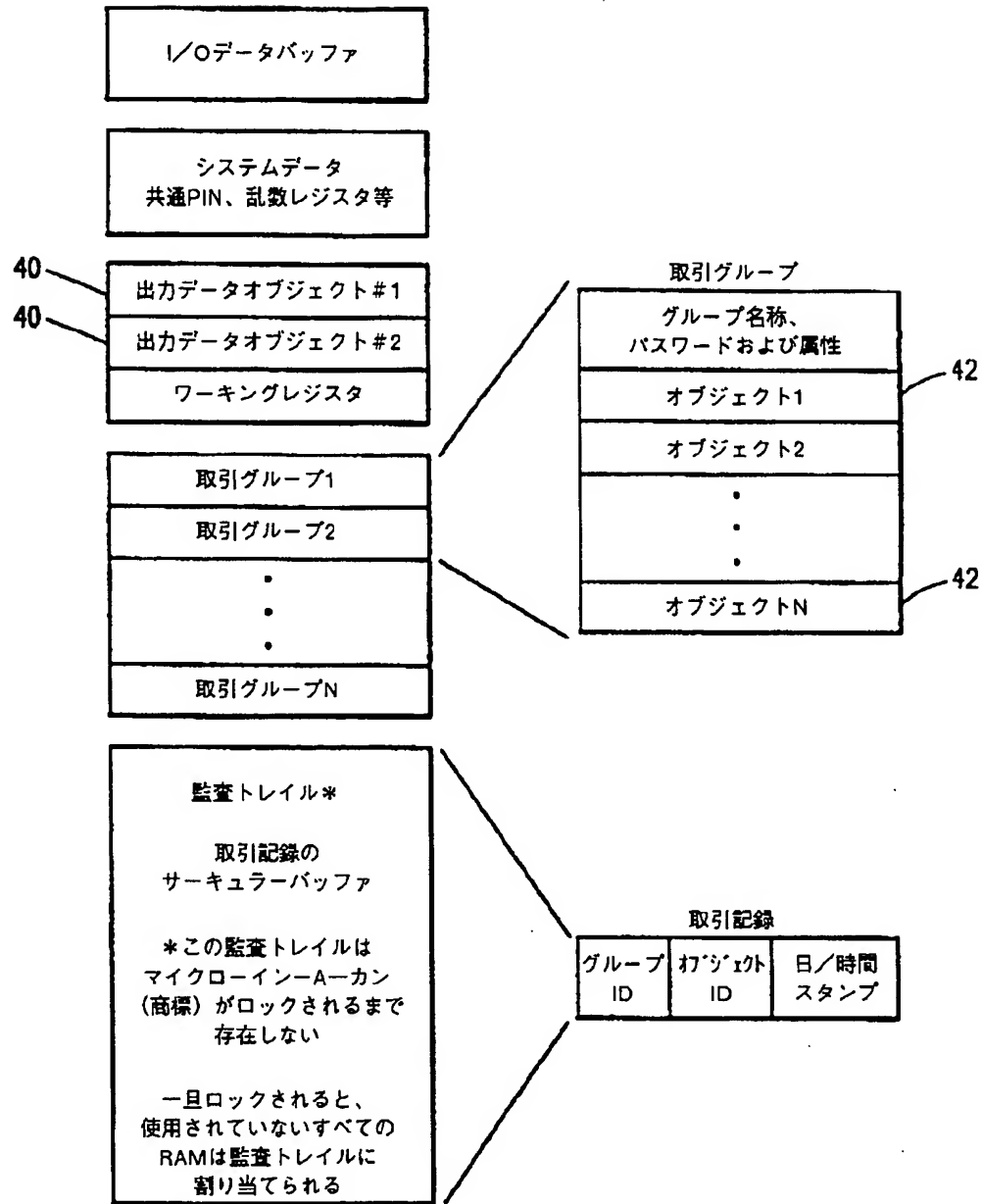


FIG. 12

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 95/15471

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 G07F7/10 G07F19/00 G06F17/60		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 458 306 A (TOSHIBA) 27 November 1991 see abstract; claims; figures 1-7 ---	1,4
Y X A	EP 0 186 981 A (IBM) 9 July 1986 see abstract; claims; figures 1-7 ---	1,4 21 8,9,13
Y	EP 0 194 839 A (TOSHIBA) 17 September 1986 see abstract; claims; figures see page 9, line 1 - page 15, line 24 see page 18, line 26 - page 19, line 23 --- -/-	1,2, 6-10, 12-14, 17,18
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
21 March 1997		02. 04. 97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 spo nl, Fax (+ 31-70) 340-3016		Authorized officer David, J

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 96/15471

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 44 06 602 A (DEUTSCHE BUNDESPOST TELEKOM) 7 September 1995	1,2, 6-10, 12-14, 17,18
A	see the whole document ---	4,21
A	EP 0 294 248 A (ELECTRONIQUE SERGE DASSAULT) 7 December 1988 see the whole document ---	1-3,6-9, 12-20
A	EP 0 624 014 A (A.M. FISCHER) 9 November 1994 see abstract; claims; figures ---	1,4,5,22
A	EP 0 337 185 A (SPA SYSPATRONIC) 18 October 1989 ---	
A	WO 93 08545 A (JONHIG) 29 April 1993 ---	
A	EP 0 172 670 A (TECHNION RESEARCH & DEVELOPMENT) 26 February 1986 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.
PCT/US 96/15471

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0458306 A	27-11-91	JP 4033085 A	04-02-92
EP 0186981 A	09-07-86	GB 2168514 A	18-06-86
		DE 3585439 A	02-04-92
		JP 61139878 A	27-06-86
		US 4731842 A	15-03-88
EP 0194839 A	17-09-86	JP 6091526 B	14-11-94
		JP 62000140 A	06-01-87
		US 4862501 A	29-08-89
DE 4406602 A	07-09-95	NONE	
EP 0294248 A	07-12-88	FR 2615638 A	25-11-88
		DE 3887207 D	03-03-94
		DE 3887207 T	26-05-94
		ES 2048211 T	16-03-94
EP 0624014 A	09-11-94	US 5422953 A	06-06-95
		AU 666424 B	08-02-96
		AU 5778194 A	17-11-94
		CA 2120665 A	06-11-94
		JP 7254897 A	03-10-95
EP 0337185 A	18-10-89	AT 123347 T	15-06-95
		DE 58909263 D	06-07-95
		ES 2072870 T	01-08-95
		US 4985921 A	15-01-91
WO 9308545 A	29-04-93	AT 145744 T	15-12-96
		AU 663739 B	19-10-95
		AU 2888692 A	21-05-93
		BR 9205416 A	17-05-94
		CA 2098481 A	17-04-93
		DE 69215501 D	09-01-97
		EP 0567610 A	03-11-93
		JP 6503913 T	28-04-94
		PL 299825 A	18-04-94
		US 5440634 A	08-08-95

Information on patient family members

PCT/US 96/15471

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0172670 A	26-02-86	JP 61094177 A	13-05-86

フロントページの続き

(51) Int. Cl. ⁶	識別記号	F I	
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 6 0 G
	6 6 0		6 6 0 F
		G 0 6 F 15/30	M
			L
		15/21	3 4 0 Z
			A

(81) 指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN

(72) 発明者 フォックス, クリストファー, ダブリュ.
 アメリカ合衆国75287 テキサス州 ダラス,
 ティムバーグレン 3847 ナンバー
 4222

THIS PAGE BLANK (USPTO)